SPLITTING OF ABELIAN VARIETIES, ELLIPTIC MINUSCULE PAIRS

V. KUMAR MURTY AND YING ZONG

1. Introduction

The following question (cf. [2], 1.1) concerns us :

Given an absolutely simple abelian variety A_K over a number field K, is there a finite extension K' of K such that $A_K \times_K L$, L any finite extension of K', specializes to simple abelian varieties at a set of places of positive Dirichlet density?

Let $t = \mathrm{Spec}(K)$, $\overline{t}$ a geometric point of t, S an open sub-scheme of the normalization of $\mathrm{Spec}(\mathbf{Z})$ in t such that $A_t = A_K$ extends to an abelian scheme A over S.

Observe that if $\mathrm{End}_t(A_t)$ is not commutative, $A_s = A \times_S s$ is not simple at any point of S with values in a finite prime field, for otherwise $\mathrm{End}_s(A_s) \otimes_{\mathbf{Z}} \mathbf{Q}$ would be a field ([4], p. 98, line 1), but the specialization homomorphism

$$sp : \mathrm{End}_t(A_t) \xleftarrow{\sim} \mathrm{End}_S(A) \hookrightarrow \mathrm{End}_s(A_s)$$

is injective.

Therefore, it is necessary, in order that the question have not a trivial negative answer, to impose $\mathrm{End}_{\overline{t}}(A_{\overline{t}}) \otimes_{\mathbf{Z}} \mathbf{Q}$ be a field.

For any prime number ℓ invertible on S, consider an ℓ-adic approach to the question :

Choose for each closed point $s \in S$ a geometric point $\overline{s}$ localized at s, and a chemin ch_s connecting $\overline{s}$ to $\overline{t}$. Let $F_s \in \pi_1(s, \overline{s})$ be the geometric Frobenius, F_s^* the image of F_s under the composition

$$\pi_1(s, \overline{s}) \to \pi_1(S, \overline{s}) \xrightarrow{ch_s} \pi_1(S, \overline{t}) \xrightarrow{\rho_{\ell,\overline{t}}} \mathrm{GL}(H^1(A_{\overline{t}}, \mathbf{Q}_\ell)),$$

where $\rho_{\ell,\overline{t}}$ is the ℓ-adic monodromy representation associated to the abelian scheme A. Write $M_\ell = \mathrm{Im}(\rho_{\ell,\overline{t}})$ for the monodromy, M_ℓ^{Zar} its Zariski closure in $\mathrm{GL}(H^1(A_{\overline{t}}, \mathbf{Q}_\ell))$. Enlarging K to a finite extension if necessary, suppose $\mathrm{End}_t(A_t) = \mathrm{End}_{\overline{t}}(A_{\overline{t}})$, and M_ℓ^{Zar} connected.

Tate's theorem applied to a closed fibre A_s,

$$\mathrm{End}_s(A_s) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell \xrightarrow{\sim} \mathrm{End}_{F_s^*}(H^1(A_{\overline{t}}, \mathbf{Q}_\ell))^{\mathrm{opposite}},$$

shows that A_s is simple if F_s^* is irreducible on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$. The subset X_ℓ of the compact ℓ-adic Lie group M_ℓ consisting of those elements irreducible on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$, is a union of conjugacy classes, and by Krasner's lemma, open in M_ℓ. By Cebotarev's density theorem, the volume of X_ℓ in the normalized Haar measure of M_ℓ equals the Dirichlet density of the set

$$\{s \in S\backslash\{t\}, F_s^* \in X_\ell\},$$

which is $\leq$ the density of

$$\{s \in S\backslash\{t\}, A_s \text{ is simple}\}.$$

Thus, the question has a positive answer, provided that X_ℓ is non-empty over any finite extension of K.

Any element of X_ℓ lies in a maximal torus of M_ℓ^{Zar} irreducible on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$. Conversely, any torus of M_ℓ^{Zar} irreducible on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$ contains an open dense subset all whose $\mathbf{Q}_\ell$-points are irreducible on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$. Since M_ℓ is open in $M_\ell^{\mathrm{Zar}}(\mathbf{Q}_\ell)$ (Bogomolov), the condition that X_ℓ be non-empty is equivalent to that some maximal torus of M_ℓ^{Zar} be irreducible on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$.

However, if $\mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell$ is not a field, even M_ℓ^{Zar} is reducible on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$, equivalently, $\Lambda/\ell\Lambda$, Λ being any $\pi_1(t, \overline{t})$-stable $\mathbf{Z}_\ell$-lattice of $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$, is a reducible $\mathbf{F}_\ell[\pi_1(t, \overline{t})]$-module, for (Faltings)

$$\mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell \xrightarrow{\sim} \mathrm{End}_{M_\ell^{\mathrm{Zar}}}(H^1(A_{\overline{t}}, \mathbf{Q}_\ell))^{\mathrm{opposite}}.$$

If, for instance, typically, $E := \mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}$ contains an abelian field of group $(\mathbf{Z}/p\mathbf{Z})^4$, p prime, or a non-solvable Galois extension of $\mathbf{Q}$, no completion $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is a field.

We assume that $\mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = E_\ell$ is a field for some prime number ℓ ; without the very restrictive assumption, there is little to say. (On the other hand, by Hilbert's irreducibility theorem, if a prime number ℓ is given, plenty totally real number fields or totally imaginary quadratic extensions of totally real fields have prescribed ℓ-adic completions.)

Then, $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$, as an E_ℓ-linear representation of M_ℓ^{Zar} or its derived group, is absolutely irreducible.

Now, at least for $\eta = \mathrm{Spec}(E_\ell)$, $G = [M_\ell^{\mathrm{Zar}}, M_\ell^{\mathrm{Zar}}]$, $V = H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$, one asks the basic question :

Let G be a semi-simple algebraic group over the spectrum η of a finite extension of $\mathbf{Q}_\ell$, $\rho_V : G \to \mathrm{GL}(V)$ an absolutely irreducible η-linear representation of finite kernel. Does some maximal torus of G act irreducibly on V?

One may assume G simply connected. Let $\overline{\eta}$ be a geometric point of η. A maximal torus $\mathfrak{T}$ is irreducible on V if and only if the weights of $V_{\overline{\eta}}$ relative to $\mathfrak{T}_{\overline{\eta}}$ are permuted transitively by $\pi_1(\eta, \overline{\eta})$. So if such a torus exists, $V_{\overline{\eta}}$ has to be minuscule.

Let $D_{\overline{\eta}}$ be the Dynkin diagram of $G_{\overline{\eta}}$, $\rho_D : \pi_1(\eta, \overline{\eta}) \to \mathrm{Aut}(D_{\overline{\eta}})$, the index, and let α_i, $i = 1, \cdots, r$, be the $\pi_1(\eta, \overline{\eta})$-orbits in $D_{\overline{\eta}}$ consisting of minuscule vertices corresponding to a minuscule representation $V = V_1 \otimes_\eta \cdots \otimes_\eta V_r$ of $G = G_1 \times_\eta \cdots \times_\eta G_r$, G_i being the simple factors. Put $D = (D_{\overline{\eta}}, \rho_D)$, $\alpha = \sum \alpha_i$.

Whether or not G has a maximal torus irreducible on V depends only on (D, α) (Theorem 2.3, Lemma 3.1) ; if G does, we call (D, α) an elliptic minuscule pair.

The main technical result of the article, Theorem 3.2, is the enumeration of elliptic minuscule pairs with connected Dynkin diagrams, which gives the essential content of the following theorem.

Theorem 1.1. *Let ℓ be a prime number. If $\mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = \mathrm{End}_{\overline{t}}(A_{\overline{t}}) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = E_\ell$ is a field, M_ℓ^{Zar} is connected, and the monodromy representation $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$ is minuscule whose associated minuscule pair over $\mathrm{Spec}(E_\ell)$ is elliptic, then A_t specializes to absolutely simple abelian varieties at a set of places of positive Dirichlet density.*

This is a consequence of what has been said and that for a set of points $s \in S \backslash \{t\}$ of density 1, $\mathrm{End}_{\overline{s}}(A_{\overline{s}})$ are commutative (cf. 2.9).

2. Elliptic minuscule pairs

2.1. A Dynkin diagram is a finite set D, equipped with the structure of a function $l : D \to \{1, 2, 3\}$ ("longueurs") and a binary relation L ("liaisons") on D, such that L is disjoint with the diagonal of $D \times D$.

Every root system has its Dynkin diagram with connected components labeled according to types as $A, B, \cdots, G_2$.

Let S be a scheme. An S-Dynkin diagram is a sheaf of sets D on S for the étale topology, locally constant, constructible, equipped with the structure of a morphism $l : D \to \{1, 2, 3\}_S$ and a sheaf of S-relations $L \subset D \times D$, L locally constant, constructible on S, such that for any geometric point s of S, the fibre D_s, with the function l_s and the relation L_s, is a Dynkin diagram.

The category of S-Dynkin diagrams is the fibre category over S of a stack in groupoids over (Sch) for the étale topology.

The monodromy representation

$$\rho_{D,s} : \pi_1(S, s) \to \mathrm{Aut}(D_s, l_s, L_s)$$

of an S-Dynkin diagram D at a geometric point $s \to S$ is the *index* of D at s.

Define $\pi_0(D)$ to be the quotient of D by the equivalence relation generated by L. Then D is a $\pi_0(D)$-Dynkin diagram.

Every reductive S-group scheme has its S-Dynkin diagram, functorial with respect to isomorphisms and compatible with base change (SGA 3, Éxposé XXIV, 3.3).

Given an S-Dynkin diagram D, if at any geometric point s of S the components of the fibre D_s are of types $A, B, \cdots, G_2$, then there is a quasi-épinglé, semi-simple, simply connected S-group scheme having D as its S-Dynkin diagram (SGA 3, Éxposé XXIV, Théorème 3.11).

Also, for any semi-simple, simply connected S-group scheme G, there exists a pair (Q, u), unique up to a unique isomorphism, consisting of a quasi-épinglé, semi-simple, simply connected S-group scheme Q and an "isomorphisme extérieur" $u \in \mathrm{Isom.ext}_S(Q, G)$ (SGA 3, Éxposé XXIV, Corollaire 3.12). The existence of u enables the identification of the S-Dynkin diagram D of Q with that of G, and permits to define the S-scheme of "isomorphismes intérieurs"

$$\underline{\mathrm{Isom.int}}_S(Q, G),$$

which is a left torsor under the adjoint group of G and a right torsor under the adjoint group of Q.

Let $T \subset B$ be the canonical maximal torus and Borel subgroup of Q, U the unipotent radical of B. Let N be the normalizer of T in Q, $W = N/T$ the Weyl group. Let

$$\pi : X \to S$$

denote the S-scheme Q/B, which is projective, smooth, with geometrically connected fibres over S.

Suppose

$$\omega : T \to \mathbf{G}_{m,S}$$

is a weight of Q with respect to T, dominant relative to the notion of positivity defined by B. Let

$$\omega_B : B \to B/U = T \xrightarrow{\omega} \mathbf{G}_{m,S}$$

be the composition ; this character, twisted by the B_X-torsor

$$Q \to Q/B = X,$$

provides a $\mathbf{G}_{m,X}$-torsor

$$Q \wedge^{B_X} \mathbf{G}_{m,X}$$

and an invertible $\mathcal{O}_X$-module

$$L_\omega = Q \wedge^{B_X} \mathbf{G}_{m,X} \wedge^{\mathbf{G}_{m,X}} \mathcal{O}_X.$$

Recall that $E_\omega = \pi_* L_\omega$ is a representation of Q on a locally free $\mathcal{O}_S$-module of finite rank, of formation compatible with any base change, and if S is the spectrum of an algebraically closed field of characteristic zero, E_ω is irreducible of highest weight ω.

In particular, to each section $\alpha \in D(S)$ of the S-Dynkin diagram D, there corresponds a fundamental representation E_α of Q of fundamental weight ω_α.

A section $\alpha \in D(S)$ is *minuscule* if the Weyl orbit

$$W\omega_\alpha \subset \underline{\mathrm{Hom}}_S(T, \mathbf{G}_{m,S})$$

is the sheaf of weights of E_α relative to T.

More generally, $\alpha = \sum_{i=1}^r \alpha_i$, $\alpha_i \in D(S)$, is *minuscule*, if each α_i is minuscule and for any geometric point s of S, $\alpha_{i,s}$ lie in distinct components of D_s. Let $W\omega_\alpha := W\omega_{\alpha_1} \times \cdots \times W\omega_{\alpha_r}$.

Definition 2.2. *Suppose S connected and $\alpha = \sum_{i=1}^r \alpha_i$ minuscule. The pair (D, α) is said to be an* elliptic minuscule pair*, or simply* elliptic*, if there is a W-torsor x on S such that*

$$x \wedge^W W\omega_\alpha$$

is a connected object in the Galois category of locally constant, constructible sheaves on S, that is, at any geometric point s of S, the image of the monodromy representation

$$\rho_{x,s} : \pi_1(S, s) \to \mathrm{Aut}((x \wedge^W W\omega_\alpha)_s)$$

acts transitively on the fibre $(x \wedge^W W\omega_\alpha)_s$. Any such W-torsor x is said to be elliptic *for (D, α).*

Theorem 2.3. *Let η be the spectrum of a completely discretely valued field of characteristic zero of finite residue field, G a semi-simple algebraic group over η of Dynkin diagram D, $\rho_V : G \to \mathrm{GL}(V)$ an absolutely irreducible representation of finite kernel. Then some maximal torus of G acts irreducibly on V if and only if V is minuscule and (D, α) is elliptic, α being the minuscule section corresponding to V.*

For the proof, we may and do assume G simply connected.

If a maximal torus $\mathfrak{T}$ of G is irreducible on V, the weights of $V_{\overline{\eta}}$ relative to $\mathfrak{T}_{\overline{\eta}}$ are permuted transitively by $\pi_1(\eta, \overline{\eta})$, a priori, all the weights have the same norm, i.e. V is minuscule.

In the following, suppose V minuscule, let $\alpha = \sum \alpha_i$, $\alpha_i \in D(\eta)$, be the corresponding section.

Lemma 2.4. *For any anisotropic maximal torus $\mathfrak{T}$ of G, of image $\mathfrak{T}^{\mathrm{ad}}$ in the adjoint group G^{ad}, the map*

$$H^1(\eta, \mathfrak{T}^{\mathrm{ad}}) \to H^1(\eta, G^{\mathrm{ad}})$$

is surjective, and $H^2(\eta, \mathfrak{T}) = 0$.

Proof. Write Z for the center of G. The extension

$$1 \to Z \to G \to G^{\mathrm{ad}} \to 1$$

induces the cohomology sequence

$$H^1(\eta, G) \to H^1(\eta, G^{\mathrm{ad}}) \xrightarrow{\partial} H^2(\eta, Z).$$

As G is simply connected, $H^1(\eta, G) = 0$. Hence

$$\partial : H^1(\eta, G^{\mathrm{ad}}) \to H^2(\eta, Z)$$

is injective.

To show

$$H^1(\eta, \mathfrak{T}^{\mathrm{ad}}) \to H^1(\eta, G^{\mathrm{ad}})$$

is surjective, it suffices to show the composition

$$\delta : H^1(\eta, \mathfrak{T}^{\mathrm{ad}}) \to H^1(\eta, G^{\mathrm{ad}}) \xrightarrow{\partial} H^2(\eta, Z)$$

is surjective.

Note that

$$\delta : H^1(\eta, \mathfrak{T}^{\mathrm{ad}}) \to H^2(\eta, Z)$$

is a coboundary of the extension

$$1 \to Z \to \mathfrak{T} \to \mathfrak{T}^{\mathrm{ad}} \to 1,$$

whose cohomology sequence

$$H^1(\eta, \mathfrak{T}^{\mathrm{ad}}) \xrightarrow{\delta} H^2(\eta, Z) \to H^2(\eta, \mathfrak{T})$$

implies

$$\delta : H^1(\eta, \mathfrak{T}^{\mathrm{ad}}) \to H^2(\eta, Z)$$

is surjective if

$$H^2(\eta, \mathfrak{T}) = 0.$$

Show $H^2(\eta, \mathfrak{T}) = 0$:

Since the Yoneda pairing

$$\mathrm{Hom}_\eta(\mathfrak{T}, \mathbf{G}_m) \times H^2(\eta, \mathfrak{T}) \to H^2(\eta, \mathbf{G}_m) \tilde{\to} \mathbf{Q}/\mathbf{Z}$$

is perfect, it needs to verify that

$$\mathrm{Hom}_\eta(\mathfrak{T}, \mathbf{G}_m) = 0,$$

which is precisely the condition that $\mathfrak{T}$ is anisotropic. □

Let the quasi-épinglé, semi-simple, simply connected algebraic group Q over η, the "isomorphisme extérieur" $u \in \mathrm{Isom.ext}_\eta(Q, G)$, and the bitorsor $\underline{\mathrm{Isom.int}}_\eta(Q, G)$ be as in (2.1).

Let $T \subset B$ be the canonical maximal torus and Borel subgroup of Q, N the normalizer of T in Q, $W = N/T$, C the center of Q, T^{ad} (resp. N^{ad}) the image of T (resp. N) in the adjoint group Q^{ad}.

Let $E_\alpha = \otimes E_{\alpha_i}$ be the minuscule representation of Q of fundamental weight ω_α.

Lemma 2.5. *1) The $Q^{\mathrm{ad}}(\eta)$-conjugacy classes of maximal tori of Q are in bijective correspondence with the elements of $H^1(\eta, N)$.*

2) The map $H^1(\eta, N) \to H^1(\eta, W)$ is injective, whose image contains the isomorphism classes of W-torsors x on η such that $x \wedge^W T$ are anisotropic.

Proof. 1) The set $(Q/N)(\eta)$ classifies the maximal tori of Q because locally on η for the étale topology they are all conjugate to T by sections of Q.

The exact sequence of pointed sets

$$Q^{\mathrm{ad}}(\eta) \to (Q/N)(\eta) \to H^1(\eta, N^{\mathrm{ad}}) \to H^1(\eta, Q^{\mathrm{ad}})$$

shows that the $Q^{\mathrm{ad}}(\eta)$-orbits in $(Q/N)(\eta)$ are in one-to-one correspondence with the elements of the kernel of

$$H^1(\eta, N^{\mathrm{ad}}) \to H^1(\eta, Q^{\mathrm{ad}}).$$

Observe that in the cohomology sequence

$$H^1(\eta, Q) \to H^1(\eta, Q^{\mathrm{ad}}) \xrightarrow{\partial} H^2(\eta, C)$$

of the extension

$$1 \to C \to Q \to Q^{\mathrm{ad}} \to 1,$$

the map

$$\partial : H^1(\eta, Q^{\mathrm{ad}}) \to H^2(\eta, C)$$

is injective, since

$$H^1(\eta, Q) = 0,$$

Q being simply connected.

Hence, the kernel of

$$H^1(\eta, N^{\mathrm{ad}}) \to H^1(\eta, Q^{\mathrm{ad}})$$

equals the kernel of the composition

$$\delta : H^1(\eta, N^{\mathrm{ad}}) \to H^1(\eta, Q^{\mathrm{ad}}) \xrightarrow{\partial} H^2(\eta, C).$$

This

$$\delta : H^1(\eta, N^{\mathrm{ad}}) \to H^2(\eta, C)$$

is a coboundary of the central extension

$$1 \to C \to N \to N^{\mathrm{ad}} \to 1.$$

From the exact sequence

$$H^1(\eta, C) \to H^1(\eta, N) \to H^1(\eta, N^{\mathrm{ad}}) \xrightarrow{\delta} H^2(\eta, C),$$

it follows that $\mathrm{Ker}(\delta)$ equals the image of

$$H^1(\eta, N) \to H^1(\eta, N^{\mathrm{ad}}).$$

To conclude $H^1(\eta, N)$ is isomorphic to this image, it needs to show that the map

$$H^1(\eta, C) \to H^1(\eta, N)$$

is 0.

By the factorization

$$H^1(\eta, C) \to H^1(\eta, T) \to H^1(\eta, N),$$

it suffices to show

$$H^1(\eta, T) = 0.$$

Prove $H^1(\eta, T) = 0$:

This follows from the identity

$$H^1(\eta, T) = H^1(D, \mathbf{G}_m)$$

(SGA 3, Éxposé XXIV, Corollaire 3.14) and Satz 90,

$$H^1(D, \mathbf{G}_m) = 0,$$

the Dynkin diagram D being representable by a scheme, finite, étale over η.

2) That

$$H^1(\eta, N) \to H^1(\eta, W)$$

is injective results from the cohomology sequence

$$H^1(\eta, T) \to H^1(\eta, N) \to H^1(\eta, W)$$

and that $H^1(\eta, T) = 0$.

The class of a W-torsor x on η lies in the image of

$$H^1(\eta, N) \to H^1(\eta, W)$$

if and only if an obstruction

$$o(x) \in H^2(\eta, x \wedge^W T)$$

vanishes.

When $x \wedge^W T$ is anisotropic, $H^2(\eta, x \wedge^W T) = 0$ (2.4). □

Lemma 2.6. *Any torus of G irreducible on V is anisotropic.*

Proof. A torus is anisotropic if and only if it has no diagonalizable sub-torus other than 1.

Recall that the kernel of the representation

$$\rho_V : G \to \mathrm{GL}(V)$$

is finite. And as G is semi-simple, $\det(\rho_V) = 1$.

If a $\mathbf{G}_m$ were in a torus of G irreducible on V, it would act on V by a character $z \mapsto z^n$, for some integer n, thus on $\det(V)$ by the character $z \mapsto z^{nd}$, $d = \dim(V)$. So $nd = 0$, i.e. $n = 0$, and $\mathbf{G}_m$ was contained in $\mathrm{Ker}(\rho_V)$. □

Lemma 2.7. *The group G has a maximal torus irreducible on V if and only if the group Q has a maximal torus irreducible on E_α.*

Proof. Suppose a maximal torus $\mathfrak{T}$ of G is irreducible on V. By (2.6), $\mathfrak{T}$ is anisotropic, and

$$H^1(\eta, \mathfrak{T}^{\mathrm{ad}}) \to H^1(\eta, G^{\mathrm{ad}})$$

is surjective (2.4). The G^{ad}-torsor

$$\underline{\mathrm{Isom.int}}_\eta(Q, G)$$

is in particular the image of a $\mathfrak{T}^{\mathrm{ad}}$-torsor, which means (SGA 3, Éxposé XXIV, Proposition 2.11) that $\mathfrak{T}$ imbeds into Q as a maximal torus and the scheme

$$\mathfrak{I} = \underline{\mathrm{Isom.int}}_\eta(Q, G; \mathrm{Id\ on\ } \mathfrak{T})$$

of "isomorphismes intérieurs" from Q to G that induce the identity automorphism on $\mathfrak{T}$, is not empty.

Let $\overline{\eta}$ be a geometric point of η. The choice of a section $\iota \in \mathfrak{I}(\overline{\eta})$ identifies the sheaves of weights of V and E_α relative to $\mathfrak{T}$. So E_α is isomorphic to V as a $\mathfrak{T}$-module, therefore is irreducible.

The other direction is proven similarly. □

2.8. Now, prove the theorem 2.3.

By (2.7), it suffices to show that (D, α) is elliptic if and only if a maximal torus of Q is irreducible on E_α.

Suppose first Q admits a maximal torus acting irreducibly on E_α.

This torus has the form $z \wedge^N T$ for an N-torsor z (2.5). Relative to it the sheaf of weights of E_α is

$$z \wedge^N W\omega_\alpha \subset z \wedge^N \underline{\mathrm{Hom}}_\eta(T, \mathbf{G}_m).$$

The condition that $z \wedge^N T$ be irreducible on E_α is equivalent to that $z \wedge^N W\omega_\alpha$ be a connected object in the Galois category of locally constant constructible sheaves on η. So $z \wedge^N W$ is an elliptic W-torsor for (D, α).

Next, suppose (D, α) elliptic, with x an elliptic W-torsor.

Let $\rho : Q \to \mathrm{GL}(E_\alpha)$ be the representation, ρ_T its restriction to T. One has $\mathrm{Ker}(\rho_T)$ is finite and $\det(\rho_T) = 1$.

The torsor x twists ρ_T to a representation

$$\rho_{x,T} : x \wedge^W T \to \mathrm{GL}(E_x)$$

with $x \wedge^W W\omega_\alpha$ as its sheaf of weights.

Hence, $\rho_{x,T}$ is irreducible, and being a twist of ρ_T, it has finite kernel and determinant 1. As in (2.6), $x \wedge^W T$ is anisotropic, thus can be imbedded into Q (2.5) ; it is the sought-for maximal torus of Q irreducible on E_α.

2.9. *Proof of the theorem 1.1.*

Frobenius F_s^*, being semi-simple on $H^1(A_{\bar{t}}, \mathbf{Q}_\ell)$, lies in a maximal torus $\mathfrak{T}(s)$ of M_ℓ^{Zar}, of eigenvalues $\chi_i(F_s^*)$, where χ_i, $1 \leq i \leq 2g$, $g = \dim(A_t)$, are the weights of $H^1(A_{\bar{t}}, \mathbf{Q}_\ell)$ with respect to $\mathfrak{T}(s)$.

If $\chi_i(F_s^*)^N = \chi_j(F_s^*)^N$, for some $i \neq j$, $N \geq 1$,

$$\chi_i(F_s^*)/\chi_j(F_s^*) \in K_s := \mathbf{Q}(\chi_1(F_s^*), \cdots, \chi_{2g}(F_s^*))$$

is a root of unity. By the purity of $\chi_i(F_s^*)$, $[K_s : \mathbf{Q}] \leq (2g)!$. The roots of unity in K_s have order $d(g)$ bounded by a constant depending only on g. The set U of elements $u \in M_\ell$ such that $u^{d(g)}$ has $2g$ distinct eigenvalues on $H^1(A_{\bar{t}}, \mathbf{Q}_\ell)$, is open in M_ℓ, stable under conjugation, of measure equal to the density of

$$\Sigma = \{s \in S\backslash\{t\}, (F_s^*)^N \text{ has } 2g \text{ distinct eigenvalues, } \forall\ N \geq 1\}.$$

The measure is 1, since the characters χ_i are all distinct.

Consider $s' \to s$, irreducible, finite, étale, of degree $N \geq 1$, $s \in \Sigma$. As $(F_s^*)^N$ has $2g$ distinct eigenvalues, $\mathrm{End}_{s'}(A_{s'})$ is commutative, for

$$\mathrm{End}_{s'}(A_{s'}) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell \xrightarrow{\sim} \mathrm{End}_{(F_s^*)^N}(H^1(A_{\bar{t}}, \mathbf{Q}_\ell))^{\mathrm{opposite}}.$$

Now A_s is isogenous to a product of simple abelian varieties A_i, $i \in I$. If one factor appears with multiplicity > 1, or if $A_i \times_s s'$ is not simple, or if $A_i \times_s s'$ and $A_j \times_s s'$ are isogenous for $i \neq j$, $\mathrm{End}_{s'}(A_{s'})$ is not commutative.

As A_t also specializes to simple abelian varieties at a set of places of density > 0, the theorem follows.

3. Simple elliptic pairs

Let S be a connected scheme, (D,α) be as in (2.2).

Suppose $\pi_0(D)=1$. Thus if D is non-constant, (D,α) can only be $({}^2A_n,\alpha_{\frac{n+1}{2}})$, n odd ≥ 3, $({}^2D_n,\alpha_1)$, $n\geq 5$, or $({}^2D_4,\alpha_i)$, $i=1,3,4$.

Let s be a geometric point of S. We write down the condition that (D,α) be elliptic.

Lemma 3.1. *1) (A_n,α_r), $r\in[1,n]$, is elliptic if and only if there is a representation*

$$\rho:\pi_1(S,s)\to\mathfrak{S}_{n+1}$$

whose image permutes transitively the subsets of $\{1,\cdots,n+1\}$ of cardinality r.

2) (B_n,α_n) is elliptic if and only if there is a representation

$$\rho:\pi_1(S,s)\to\mathrm{GL}_n(\mathbf{Z})$$

whose image lies in the group generated by the diagonal matrices and monomial matrices, and acts transitively on

$$\{\pm e_1\pm\cdots\pm e_n\},$$

where $e_1,\cdots,e_n$ denotes the standard base of $\mathbf{Z}^n$.

3) (C_n,α_1) is elliptic if and only if there is a representation

$$\rho:\pi_1(S,s)\to\mathrm{GL}_n(\mathbf{Z})$$

whose image lies in the group generated by the diagonal matrices and monomial matrices, and acts transitively on

$$\{e_1,\cdots,e_n,-e_1,\cdots,-e_n\},$$

where $e_1,\cdots,e_n$ denotes the standard base of $\mathbf{Z}^n$.

4) (D_n,α_1) is elliptic if and only if there is a representation

$$\rho:\pi_1(S,s)\to\mathrm{GL}_n(\mathbf{Z})$$

whose image lies in the group generated by the diagonal matrices of determinant 1 and monomial matrices, and acts transitively on

$$\{e_1,\cdots,e_n,-e_1,\cdots,-e_n\},$$

where $e_1,\cdots,e_n$ denotes the standard base of $\mathbf{Z}^n$.

5) (D_n,α_{n-1}) (resp. (D_n,α_n)) is elliptic if and only if there is a representation

$$\rho:\pi_1(S,s)\to\mathrm{GL}_n(\mathbf{Z})$$

whose image lies in the group generated by the diagonal matrices of determinant 1 *and monomial matrices, and permutes transitively the vectors*

$$s_1e_1 + \cdots + s_ne_n,$$

where $s_i \in \{1, -1\}$, $s_1 \cdots s_n = -1$ *(resp.* $s_1 \cdots s_n = 1$*), and* $e_1, \cdots, e_n$ *denotes the standard base of* $\mathbf{Z}^n$.

6) (E_6, α_i), $i = 1, 6$, *is elliptic if and only if there is a representation*

$$\rho : \pi_1(S, s) \to \mathrm{O}(\mathbf{F}_2^6, q)$$

whose image permutes transitively the non-zero singular vectors in $\mathbf{F}_2^6$, *where* q *is the quadratic form such that*

$$q(e_i) = q(f_j) = 1,\ q(e_i + e_j) = q(f_i + f_j) = 0,\ q(e_i + f_j) = \delta_{ij},$$

e_i, f_j, $1 \leq i, j \leq 3$, *is a base of* $\mathbf{F}_2^6$, $\delta_{ij} = 1$, *if* $i = j$, *and* 0, *if* $i \neq j$.

7) (E_7, α_7) *is elliptic if and only if there is a representation*

$$\rho : \pi_1(S, s) \to \{1, -1\} \times \mathrm{Sp}_6(\mathbf{F}_2)$$

whose image acts transitively on $\{1, -1\} \times (\mathrm{Sp}_6(\mathbf{F}_2)/\mathrm{O}(q))$, q *being the quadratic form on* $\mathbf{F}_2^6$ *with*

$$q(e_i) = q(f_j) = 1,\ q(e_i + e_j) = q(f_i + f_j) = 0,\ q(e_i + f_j) = \delta_{ij},$$

where e_i, f_j *is the standard symplectic base of* $\mathbf{F}_2^6$, $\delta_{ij} = 1$, *if* $i = j$, *and* 0, *if* $i \neq j$.

8) $({}^2A_n, \alpha_{\frac{n+1}{2}})$, n *odd* ≥ 3, *is elliptic if and only if there is a representation*

$$\rho = (\rho_1, \rho_2) : \pi_1(S, s) \to \{1, -1\} \times \mathfrak{S}_{n+1}$$

whose image permutes transitively the subsets of $\{1, \cdots, n+1\}$ *of cardinality* $(n+1)/2$, *and whose component* ρ_1 *is the index of* ${}^2A_n$. *Here* $-1 : Y \mapsto \{1, \cdots, n+1\} \backslash Y$, *for any* $Y \subset \{1, \cdots, n+1\}$ *of cardinality* $(n+1)/2$.

9) $({}^2D_n, \alpha_1)$, $n \geq 5$, *or* $({}^2D_4, \alpha_i)$, $i = 1, 3, 4$, *is elliptic if and only if there is a representation*

$$\rho : \pi_1(S, s) \to \mathrm{GL}_n(\mathbf{Z})$$

whose image acts transitively on $\{\pm e_1, \cdots, \pm e_n\}$ *and lies in the group* $\mathfrak{W}$ *generated by the diagonal matrices and monomial matrices, and such that the composition*

$$\pi_1(S, s) \xrightarrow{\rho} \mathfrak{W} \to \mathfrak{W}/\mathfrak{W}_1 = \{1, -1\}$$

is the index of ${}^2D_n$, *where* $\mathfrak{W}_1$ *is the subgroup of* $\mathfrak{W}$ *generated by the diagonal matrices of determinant* 1 *and monomial matrices, and where* $e_1, \cdots, e_n$ *denotes the standard base of* $\mathbf{Z}^n$.

Proof. Let R be the root system of Q with respect to T.

The extension

$$1 \to W \to \underline{\mathrm{Aut}}_S(R) \to \underline{\mathrm{Aut}}_S(D) \to 1,$$

with its cohomology sequence

$$H^1(S, W) \to H^1(S, \underline{\mathrm{Aut}}_S(R)) \to H^1(S, \underline{\mathrm{Aut}}_S(D)),$$

shows that an S-form R' of R is equal to some $x \wedge^W R$ for a W-torsor x if and only if R' has Dynkin diagram isomorphic to D, or equivalently, if and only if the composition

$$\pi_1(S, s) \xrightarrow{\rho_{R',s}} \mathrm{Aut}(R_s) \to \mathrm{Aut}(D_s)$$

is the index of D at s, where the monodromy representation associated to R' at s is written as $\rho_{R',s}$.

Given a $R' = x \wedge^W R$, the monodromy $\mathrm{Im}(\rho_{R',s})$ normalizes the weights $W_s\omega_\alpha$, and the condition "x is an elliptic W-torsor for (D, α)" can be translated as "$\mathrm{Im}(\rho_{R',s})$ is transitive on $W_s\omega_\alpha$".

If D is constant, W is constant. The class of a W-torsor x on S is a W-conjugacy class of representations $\rho : \pi_1(S, s) \to W$.

Type by type,

1)–6), 8)–9) the description of $\mathrm{Aut}(R_s)$, the Weyl groups, the minuscule vertices α, and the weights $W\omega_\alpha$, for (A_n, α_r), (B_n, α_n), (C_n, α_1), (D_n, α_i), $i = 1, n-1, n$, (E_6, α_i), $i = 1, 6$, $({}^2A_n, \alpha_{\frac{n+1}{2}})$, $({}^2D_n, \alpha_1)$, $({}^2D_4, \alpha_i)$, $i = 1, 3, 4$, is standard.

7) given a root system of base $\{\alpha_1, \cdots, \alpha_7\}$, of root lattice $Q(E_7)$, weight lattice $P(E_7)$, then $2P(E_7) \subset Q(E_7)$, and $E = Q(E_7)/2P(E_7)$ is a 6-dimensional $\mathbf{F}_2$-vector space on which the Killing form $(,)$ induces a symplectic form. The Weyl group $W(E_7)$ maps onto $\mathrm{Sp}(E)$ with kernel $\{1, -1\}$, where -1 has maximal length relative to $\{\alpha_1, \cdots, \alpha_7\}$. The central extension

$$1 \to \{1, -1\} \to W(E_7) \to \mathrm{Sp}(E) \to 1$$

splits. Let E_6 be the sub-system of base $\{\alpha_1, \cdots, \alpha_6\}$; its roots

$$e_1 = \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4 + \alpha_5 + \alpha_6,$$

$$e_2 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5,$$

$$e_3 = \alpha_2 + \alpha_4,$$

$$f_1 = \alpha_1 + \alpha_3 + \alpha_4,$$

$$f_2 = \alpha_4 + \alpha_5 + \alpha_6,$$

$$f_3 = \alpha_3 + \alpha_4 + \alpha_5$$

satisfy the orthogonality relations

$$(e_i, e_j) = 2\delta_{ij},\ (f_i, f_j) = 2\delta_{ij},\ (e_i, f_j) = \delta_{ij},$$

and their images in E are a symplectic base. Consequently,

$$F = Q(E_6)/2Q(E_6) \xrightarrow{\sim} Q(E_7)/2P(E_7) = E$$

is a bijection, where $Q(E_6)$ is the root lattice of E_6. When F is equipped with the quadratic form $q = \frac{1}{2}(,)$, $W(E_6)$ is identified with $\mathrm{O}(q)$, and $W(E_7)\omega_7 = W(E_7)/W(E_6) = \{1, -1\} \times (\mathrm{Sp}(E)/\mathrm{O}(q))$. □

Theorem 3.2. *Let S be the spectrum of a complete discrete valuation ring, of generic point η of characteristic zero, of closed point s, $k(s)$ finite, of characteristic ℓ. Then the elliptic minuscule pairs (D, α) over η with $\pi_0(D) = 1$ are*

A) (A_n, α_1), (A_n, α_n); (A_{ℓ^d-1}, α_2), $(A_{\ell^d-1}, \alpha_{\ell^d-2})$, $d \geq 1$; (A_{p-1}, α_2), (A_{p-1}, α_{p-2}), p prime $\equiv 1$ mod 4, $\mathrm{Card}(k(s))$ mod p generates $\mathbf{F}_p^\times$; (A_{p-1}, α_2), (A_{p-1}, α_{p-2}), p prime $\equiv 3$ mod 4, $\mathrm{Card}(k(s))$ mod p generates $\mathbf{F}_p^\times$ or $(\mathbf{F}_p^\times)^2$; (A_7, α_3), (A_7, α_5), $\ell = 2$; (A_{31}, α_3), (A_{31}, α_{29}), $\ell = 2$, $5 \nmid [s : \mathbf{F}_2]$.

${}^2A$) $({}^2A_3, \alpha_2)$; $({}^2A_5, \alpha_3)$, either $\ell = 5$, or $(\ell, 5) = 1$, $\mathrm{Card}(k(s))$ mod 5 generates $\mathbf{F}_5^\times$, ${}^2A_5$ is ramified over S.

B) (B_3, α_3); (B_4, α_4); (B_n, α_n), $n \geq 5$, $\ell = 2$.

C) (C_n, α_1), $n \geq 2$.

D) (D_n, α_1), n even ≥ 4; (D_n, α_1), n odd ≥ 5, $\ell = 2$; (D_5, α_4), (D_5, α_5); (D_6, α_5), (D_6, α_6), $\ell = 2$, or $\ell \equiv 5$ mod 8, $[s : \mathbf{F}_\ell]$ odd; (D_n, α_{n-1}), (D_n, α_n), $n \geq 7$, $\ell = 2$.

${}^2D$) $({}^2D_n, \alpha_1)$.

E_6) (E_6, α_1), (E_6, α_6), $\ell = 3$ or $\mathrm{Card}(k(s)) \equiv \pm 4$ mod 9.

E_7) (E_7, α_7), $\ell = 2$.

This list is justified in the remaining sections.

4. Two lemmas

Let S be the spectrum of a complete discrete valuation ring, of generic point η of characteristic zero, of closed point s, $k(s)$ finite, of characteristic ℓ.

Lemma 4.1. *Let d be an integer ≥ 1, $\zeta \in \mathrm{GL}_d(\mathbf{F}_\ell)$ such that*

$$\zeta : e_1 \mapsto e_2,\ e_2 \mapsto e_3,\ \cdots,\ e_d \mapsto e_1,$$

where $e_1, \cdots, e_d$ is the standard base of $\mathbf{F}_\ell^d$.

The semi-direct product $\langle\zeta\rangle\mathbf{F}_\ell^d$ is a quotient of $\pi_1(\eta,\overline{\eta})$. If $(\ell,d)=1$ and V is an irreducible $\mathbf{F}_\ell$-linear representation of $\langle\zeta\rangle$, then $\langle\zeta\rangle V$ is a quotient of $\pi_1(\eta,\overline{\eta})$.

Proof. Let $\eta'\to\eta$ be connected, unramified over S of degree d. Let S' be the normalization of S in η', $s'\in S'$ the closed point, $\zeta\in\mathrm{Gal}(\eta'/\eta)$ a generator, $\pi\in\Gamma(\mathcal{O}_S)$ a uniformizer, and $u'\in\Gamma(\mathcal{O}_{S'})^\times$ such that the images of $u',\zeta(u'),\cdots,\zeta^{d-1}(u')$ in $k(s')$ are a normal base over $k(s)$.

Then

$$\eta'[x_1,\cdots,x_d]/(x_1^\ell-x_1-\zeta(u')\pi^{-1},\cdots,x_d^\ell-x_d-\zeta^d(u')\pi^{-1})$$

is Galois over η of group $\langle\zeta\rangle\mathbf{F}_\ell^d$. If $(\ell,d)=1$, $\langle\zeta\rangle V$ is a quotient of $\langle\zeta\rangle\mathbf{F}_\ell^d$, thus is a quotient of $\pi_1(\eta,\overline{\eta})$. □

Lemma 4.2. *Let p be a prime number different from ℓ.*

1) If an $\mathbf{F}_p$-vector space V is normal in a group $\mathfrak{G}$ such that $\mathfrak{G}$ acts irreducibly by conjugation on V, then $\mathfrak{G}$ is a quotient of $\pi_1(\eta,\overline{\eta})$ only if $\dim V=1$.

2) There is a unique group of affine linear transformations of $\mathbf{F}_p$ that contains all the translations and is a quotient of $\pi_1(\eta,\overline{\eta})$ ramified over S. This group has cardinality pd, where d is the order of the element $\mathrm{Card}(k(s))$ *mod p in $\mathbf{F}_p^\times$.*

Proof. 1) Suppose $\mathfrak{G}$ is a quotient of $\pi_1(\eta,\overline{\eta})$, with inertia group $\mathfrak{R}$, wild inertia subgroup $\mathfrak{P}$. The intersection $V\cap\mathfrak{R}$, being normal in $\mathfrak{G}$, is a $\mathfrak{G}$-module. Thus, $V\cap\mathfrak{R}=1$ or V.

If $V\cap\mathfrak{R}=1$, $V\hookrightarrow\mathfrak{G}/\mathfrak{R}$, so V is cyclic.

If $V\cap\mathfrak{R}=V$, as $V\cap\mathfrak{P}=1$, then $V\hookrightarrow\mathfrak{R}/\mathfrak{P}$, which also implies V is cyclic.

2) Let $\tau:x\mapsto x+1$, $x\in\mathbf{F}_p$. For any $a\in\mathbf{F}_p^\times$, let $\sigma_a:x\mapsto ax$, $x\in\mathbf{F}_p$. In the group of affine linear transformations of $\mathbf{F}_p$, $\langle\tau\rangle$ is its own centralizer.

Suppose for some $z\in\mathbf{F}_p^\times$, $\langle\tau,\sigma_z\rangle$ is a ramified quotient of $\pi_1(\eta,\overline{\eta})$; let $\mathfrak{R}$ be its inertia subgroup, $\mathfrak{P}$ the wild inertia subgroup.

Show $\mathfrak{P}=1$: for, $\mathfrak{P}$ intersects $\langle\tau\rangle$ in 1, thus commutes with τ, thus is contained in $\langle\tau\rangle$, i.e. $=1$.

The group $\mathfrak{R}=\mathfrak{R}/\mathfrak{P}$ is cyclic. And, $\mathfrak{R}\cap\langle\tau\rangle=1$ or $\langle\tau\rangle$; in any case, $\mathfrak{R}$ commutes with τ, hence is a subgroup of $\langle\tau\rangle$, hence $\mathfrak{R}=\langle\tau\rangle$.

Write $\pi_1^t(\eta,\overline{\eta})$ for the maximal tame-along-s quotient of $\pi_1(\eta,\overline{\eta})$. From its structure,

$$\pi_1^t(\eta,\overline{\eta})=\langle\tau,\sigma|\ \sigma\tau\sigma^{-1}=\tau^q\rangle,$$

where $q = \mathrm{Card}(k(s))$, it follows that $\langle \sigma_z \rangle$ is generated by $\sigma_{z'}$, $z' := \mathrm{Card}(k(s)) \bmod p$. Now, 2) is clear. □

5. Type A

Let (S, η, s), $\mathrm{char}(s) = \ell$, be as in §4.

Proposition 5.1. *For any integer $n \geq 1$, (A_n, α_1), (A_n, α_n) are elliptic over η.*

Proof. The subgroup of $\mathfrak{S}_{n+1}$ generated by $(12 \cdots n+1)$ is transitive on $\{1, \cdots, n+1\}$ and on the collection of subsets of $\{1, \cdots, n+1\}$ of cardinality n. As $\langle (12 \cdots n+1) \rangle = \mathbf{Z}/(n+1)\mathbf{Z}$ is a quotient of $\pi_1(\eta, \overline{\eta})$, the pairs (A_n, α_i), $i = 1, n$, are elliptic over η, (3.1), 1). □

Lemma 5.2. *Let X be a finite set of cardinality $q \geq 4$, $\mathfrak{G}$ a solvable subgroup of* $\mathrm{Aut}(X)$ *permuting transitively the subsets of X of cardinality r, $2 \leq r \leq q/2$. Then $r < 4$.*

1) If $r = 2$, $\mathfrak{G}$ is 2-transitive on X, unless $X = \mathbf{F}_q$, $q \equiv 3$ mod 4, and $\mathfrak{G}$ is the group of transformations

$$x \mapsto a\sigma(x) + b,\ x \in \mathbf{F}_q,\ a \in (\mathbf{F}_q^\times)^2,\ b \in \mathbf{F}_q,\ \sigma \in \mathrm{Gal}(\mathbf{F}_q/k)$$

where k is a subfield of $\mathbf{F}_q$.

2) If $r = 3$, $X = \mathbf{F}_{32}$ or $\mathbf{F}_8$. If $X = \mathbf{F}_{32}$, $\mathfrak{G}$ consists of all affine semi-linear transformations of X. If $X = \mathbf{F}_8$, $\mathfrak{G}$ consists of either all affine semi-linear transformations or only the affine linear transformations of X.

Proof. That $r < 4$, as well as 2), is extracted from [1], p. 402–403.

If $r = 2$ and $\mathfrak{G}$ is not 2-transitive on X, then by *loc.cit*, $X = \mathbf{F}_{p^d}$, p prime $\equiv 3$ mod 4, d is odd, $\mathfrak{G} = \mathfrak{L}\mathbf{F}_p^d$, $\mathfrak{L} \leq \mathrm{GL}_d(\mathbf{F}_p)$, $\mathrm{Card}(\mathfrak{L})$ is odd. In this situation, $-1 : x \mapsto -x$, $x \in X$, normalizes $\mathfrak{G}$, $\{1, -1\}\mathfrak{G}$ is 2-transitive on X, and 1) follows from the well-known classification of 2-transitive solvable permutation groups. □

Corollary 5.3. *If $4 \leq r \leq (n+1)/2$, (A_n, α_r), (A_n, α_{n+1-r}) are not elliptic over η. The pairs (A_n, α_3), (A_n, α_{n-2}) are elliptic over η only if $n = 7$ or 31. The pairs (A_n, α_2), (A_n, α_{n-1}) are elliptic over η only if $n = p^d - 1$, p prime, $d \geq 1$.*

Proof. This is immediate from (5.2), (3.1), 1). □

Proposition 5.4. *Let p be a prime number, $d \geq 1$, $n = p^d - 1$. Then (A_n, α_2), (A_n, α_{n-1}) are elliptic over η if $p = \ell$, and only if $p = \ell$, when $d \geq 2$.*

Proof. Any solvable subgroup of $\mathfrak{S}_{n+1}$ transitive on the collection of subsets of $\{1, \cdots, n+1\}$ of cardinality 2 is of the form $\mathfrak{G} = \mathfrak{L}\mathbf{F}_p^d$, where $\mathfrak{L}$ is a subgroup of $\mathrm{GL}_d(\mathbf{F}_p)$ irreducible on $\mathbf{F}_p^d$. When $d \geq 2$, by (4.2), 1), $\mathfrak{G}$ is a quotient of $\pi_1(\eta, \overline{\eta})$ only if $p = \ell$, therefore, (A_n, α_2), as well as (A_n, α_{n-1}), is elliptic only if $p = \ell$, (3.1), 1).

Suppose $p = \ell$. The group of affine linear transformations of $\mathbf{F}_{\ell^d} = \{1, \cdots, n+1\}$ is 2-transitive, and is a quotient of $\pi_1(\eta, \overline{\eta})$ (4.1), thus, (A_n, α_2), (A_n, α_{n-1}) are elliptic. □

Proposition 5.5. *Let p be an odd prime different from ℓ, $n = p-1$. For $p \equiv 1$ mod 4, (A_n, α_2), (A_n, α_{n-1}) are elliptic over η if and only if* $\mathrm{Card}(k(s))$ *mod p generates $\mathbf{F}_p^\times$. For $p \equiv 3$ mod 4, (A_n, α_2), (A_n, α_{n-1}) are elliptic over η if and only if* $\mathrm{Card}(k(s))$ *mod p generates a subgroup of $\mathbf{F}_p^\times$ of index ≤ 2.*

Proof. The pairs (A_n, α_2), (A_n, α_{n-1}) are elliptic over η if and only if some representation $\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{S}_p$ has image transitive on the collection of 2-point subsets of $\{1, \cdots, p\} = \mathbf{F}_p$, (3.1), 1).

By (5.2), 1), and the classification of 2-transitive solvable permutation groups of degree p, the image of ρ has to be either the group of all affine linear transformations of $\mathbf{F}_p$, or, if $p \equiv 3$ mod 4, the group of affine linear transformations of $\mathbf{F}_p$ generated by the translations and the scalar multiplications $x \mapsto ax$, $a \in (\mathbf{F}_p^\times)^2$.

Now, (4.2), 2) applies. □

Proposition 5.6. *The pairs (A_7, α_3), (A_7, α_5) are elliptic over η if and only if s is of characteristic* 2.

Proof. Either of the two solvable subgroups of $\mathfrak{S}_8$ transitive on the collection of 3-point subsets of $\{1, \cdots, 8\} = \mathbf{F}_8$ contains an $\mathbf{F}_8$, (5.2), 2). So (A_7, α_3), (A_7, α_5) are elliptic over η only if s is of characteristic 2, (3.1), 1).

If $\mathrm{char}(s) = 2$, the group of affine transformations of $\mathbf{F}_8$ is a quotient of $\pi_1(\eta, \overline{\eta})$, (4.1), therefore, (A_7, α_3), (A_7, α_5) are elliptic over η, (3.1), 1). □

Proposition 5.7. *The pairs (A_{31}, α_3), (A_{31}, α_{29}) are elliptic over η if and only if s is of characteristic* 2 *and* $5 \nmid [s : \mathbf{F}_2]$.

Proof. The pairs (A_{31}, α_3), (A_{31}, α_{29}) are elliptic over η if and only if the group $\mathfrak{G}$ of affine semi-linear transformations of $\mathbf{F}_{32}$ is a quotient of $\pi_1(\eta, \overline{\eta})$, (3.1), 1), (5.2), 2).

As $\mathfrak{G}$ contains $\mathbf{F}_{32}$, it is a quotient of $\pi_1(\eta, \overline{\eta})$ only if s is of characteristic 2.

Suppose $\mathrm{char}(s) = 2$.

Evidently, when $\mathfrak{G}$ is a Galois group, its wild inertia subgroup must consist of all translations, its inertia subgroup all affine linear transformations, and the group $\mathfrak{G}^t$, generated by the Frobenius and scalar multiplications, be isomorphic to the maximal tame quotient of $\mathfrak{G}$.

By (4.2), 2), $\mathfrak{G}^t$ is a quotient of $\pi_1(\eta, \overline{\eta})$ if and only if $\mathrm{Card}(k(s))$ mod 31 is of order 5 in $\mathbf{F}_{31}^{\times}$, or equivalently, $5 \nmid [s : \mathbf{F}_2]$, for $\mathrm{Card}(k(s)) = 2^{[s:\mathbf{F}_2]}$ and 2 is of order 5 in $\mathbf{F}_{31}^{\times}$.

Suppose $5 \nmid [s : \mathbf{F}_2]$.

Let $\eta' \to \eta$ be connected, unramified over S of degree 5, let S' be the normalization of S in η', $s' \in S'$ the closed point, $\zeta \in \mathrm{Gal}(\eta'/\eta)$ a generator, $\pi \in \Gamma(\mathcal{O}_S)$ a uniformizer, and $u' \in \Gamma(\mathcal{O}_{S'})^{\times}$ such that the images of $u', \zeta(u'), \cdots, \zeta^4(u')$ in $k(s')$ form a normal base over $k(s)$.

Then

$$\eta'[z, x_1, \cdots, x_5]/(z^{31} - \pi, x_1^2 - 1 - z\zeta(u'), \cdots, x_5^2 - 1 - z\zeta^5(u'))$$

is Galois over η of group $\mathfrak{G}$. □

6. Type ^2A

Lemma 6.1. *Let d be an integer ≥ 1, X a set with $2d-1$ elements, $\mathfrak{G}$ a solvable subgroup of $\mathrm{Aut}(X)$ permuting transitively the subsets of X of cardinality d. Then $X, \mathfrak{G}$ are*

1) $X = 1$, $\mathfrak{G} = 1$.

2) $X = \{1, 2, 3\}$, $\mathfrak{G} = \mathfrak{S}_3$ or $\mathfrak{A}_3$.

3) $X = \mathbf{F}_5$, $\mathfrak{G}$ consists of all affine linear transformations

$$A_{a,b} : x \mapsto ax + b,\ x \in \mathbf{F}_5,\ a \in \mathbf{F}_5^{\times},\ b \in \mathbf{F}_5.$$

Proof. If $d = 1$, $X = 1$, $\mathfrak{G} = 1$, hence 1). Suppose $d > 1$.

Show $\mathfrak{G}$ is transitive on X: otherwise, some $\mathfrak{G}$-orbit, say O, has cardinality $< d$. Complement O to a set Y with d elements. Then $O = gO \subset gY$, $\forall\ g \in \mathfrak{G}$, that is, O is contained in every subset of X of cardinality d. But as $\mathrm{Card}(X \backslash O) > (2d-1) - d = d-1$, $X \backslash O$ contains a set Y' with d elements, which is disjoint with O.

Fix a point $o \in X$, let $\mathfrak{G}_o$ be its stabilizer in $\mathfrak{G}$.

Show $\mathfrak{G}_o$ is a maximal subgroup of $\mathfrak{G}$: assume $\mathfrak{G}_o < \mathfrak{H} < \mathfrak{G}$, for a group $\mathfrak{H}$. Then $1 < (\mathfrak{G} : \mathfrak{H}), (\mathfrak{H} : \mathfrak{G}_o) < d$, because

$$(\mathfrak{G} : \mathfrak{H})(\mathfrak{H} : \mathfrak{G}_o) = (\mathfrak{G} : \mathfrak{G}_o) = \mathrm{Card}(\mathfrak{G}.o) = \mathrm{Card}(X) = 2d - 1.$$

As $\mathfrak{H}.o \simeq \mathfrak{H}/\mathfrak{G}_o$, $X \backslash (\mathfrak{H}.o)$ has cardinality $> (2d-1) - d = d - 1$. Pick a $Y \subset X \backslash (\mathfrak{H}.o)$ with d elements so that $gY \cap g\mathfrak{H}.o = \emptyset$, $\forall\ g \in \mathfrak{G}$. Hence any subset of X of cardinality d is disjoint with some $g\mathfrak{H}.o$. But if $\mathfrak{R}$ is a set of representatives for $\mathfrak{G}/\mathfrak{H}$, as $\mathrm{Card}(\mathfrak{R}.o) \leq \mathrm{Card}(\mathfrak{R}) = (\mathfrak{G} : \mathfrak{H}) < d$, a set $Y' \supset \mathfrak{R}.o$ with d elements intersects all $g\mathfrak{H}.o$, $g \in \mathfrak{G}$.

Show $\mathfrak{G}_o$ does not contain normal subgroups of $\mathfrak{G}$ other than 1: given $\mathfrak{N} \leq \mathfrak{G}_o$, $\mathfrak{N}$ normal in $\mathfrak{G}$, then $\mathfrak{N}g.o = g\mathfrak{N}.o = g.o$, $\forall\ g \in \mathfrak{G}$, i.e. $\mathfrak{N}$ fixes pointwise $\mathfrak{G}.o = X$. So $\mathfrak{N} = 1$.

Let $\mathfrak{U}$ be the last term > 1 in the derived series of $\mathfrak{G}$. Since $\mathfrak{G}$ is solvable, $[\mathfrak{U}, \mathfrak{U}] = 1$, i.e. $\mathfrak{U}$ is abelian, thus is a $\mathfrak{G}$-module. Let $V \subset \mathfrak{U}$ be a simple sub-$\mathfrak{G}$-module ; it is an $\mathbf{F}_p$-vector space for a prime number p. Let $f = \dim V$.

Show $V\mathfrak{G}_o = \mathfrak{G}$: since V is not a subgroup of $\mathfrak{G}_o$, $V\mathfrak{G}_o$ contains $\mathfrak{G}_o$ properly. So $V\mathfrak{G}_o = \mathfrak{G}$, for $\mathfrak{G}_o$ is maximal in $\mathfrak{G}$.

Show $V \cap \mathfrak{G}_o = 1$: the group $V \cap \mathfrak{G}_o$ is normalized by $\mathfrak{G}_o$ and by V, V being abelian, thus by $V\mathfrak{G}_o = \mathfrak{G}$. Hence, $V \cap \mathfrak{G}_o$ is a sub-$\mathfrak{G}$-module of V, and is different from V, therefore is 1.

Show $V \to X$, $v \mapsto v.o$, is a bijection : it is surjective because $X = \mathfrak{G}.o = V\mathfrak{G}_o.o = V.o$. It is injective because if $v.o = v'.o$, then $v^{-1}v' \in V \cap \mathfrak{G}_o = 1$, that is, $v = v'$.

Now, $p^f = \mathrm{Card}(V) = \mathrm{Card}(X) = 2d - 1$, so $p > 2$.

Show the representation $\mathfrak{G}_o \to \mathrm{GL}(V)$, $g \mapsto \mathrm{int}(g)$, is faithful : if $g \in \mathfrak{G}_o$ and $\mathrm{int}(g) = 1$, then $gv.o = gvg^{-1}.o = \mathrm{int}(g)(v).o = v.o$, $\forall\ v \in V$, i.e. g stabilizes each point of $V.o = X$. So $g = 1$.

Let p' be a prime number with $d < p' < 2d$ (Bertrand's postulate).

Show $p' = p$: suppose $p' \neq p$. Note that p' divides $\binom{2d-1}{d}$, the number of subsets of X of cardinality d, thus divides $\mathrm{Card}(\mathfrak{G}) = p^f\ \mathrm{Card}(\mathfrak{G}_o)$, thus divides $\mathrm{Card}(\mathfrak{G}_o)$, then divides $\mathrm{Card}(\mathrm{GL}(V))$. So p' divides $p^i - 1$, for some $i = 1, \cdots, f$, i.e. $p' = p^i - 1$, since $p^f - 1 = 2d - 2 < 2p' - 2$. But p' is odd, $p^i - 1$ is even.

Show $f = 1$: it is because $p^f = 2d - 1 < 2p' - 1 = 2p - 1$.

Show $d \leq 3$: one has the division

$$\binom{2d-1}{d} \mid \mathrm{Card}(\mathfrak{G}) \mid p.\mathrm{Card}(\mathrm{GL}(V)) = p(p-1) = (2d-1)(2d-2).$$

If $d = 4$, $\binom{2d-1}{d} = 35$ does not divide $(2d-1)(2d-2) = 42$. If $d \geq 5$, $\binom{2d-1}{d} > (2d-1)(2d-2)$.

If $d = 2$, $X = \{1, 2, 3\}$. As $\mathfrak{G}$ is transitive on X, it may be $\mathfrak{S}_3$ or $\mathfrak{A}_3$. Both do permute transitively the 2-point subsets of X, hence 2).

If $d = 3$, $X \simeq V$ has 5 elements, 10 subsets of cardinality 3. Since $\mathfrak{G} \leq V.\mathrm{GL}(V)$, Card$(\mathfrak{G})$ divides 20, thus Card$(\mathfrak{G}) = 20$ or 10. Accordingly, $\mathfrak{G}$ may be $V.\mathrm{GL}(V)$, the group of affine linear transformations of $V = \mathbf{F}_5$, or its subgroup $\mathfrak{H}$ consisting of those $A_{a,b} : x \mapsto ax + b$, such that $a \in (\mathbf{F}_5^\times)^2$.

The group $V.\mathrm{GL}(V)$ is transitive on the 3-point subsets of X, for it is 2-transitive on X : given $u, v \in \mathbf{F}_5$, $u \neq v$, there is an affine linear transformation $A_{a,b} : x \mapsto ax + b$ such that $A_{a,b}(0) = u$, $A_{a,b}(1) = v$. Indeed, $b = u$, $a = v - u$.

The group $\mathfrak{H}$ permutes the 2-point subsets of X in two orbits, namely, the collection of $\{u, v\} \subset X$, where respectively $u - v$ is or is not a square of $\mathbf{F}_5^\times$. So on the 3-point subsets of X, $\mathfrak{H}$ has two orbits as well. Therefore, when $d = 3$, $\mathfrak{G} = V.\mathrm{GL}(V)$, hence 3). □

Now, suppose given an integer $d \geq 1$, a set X with $2d$ elements, a solvable subgroup $\mathfrak{G}$ of Aut(X) permuting the subsets of X of cardinality d in 2 orbits.

Lemma 6.2. *If $\mathfrak{G}$ is not transitive on X, 1) or 2) or 3) hold :*

1) $X = \{o, 1\}$, $\mathfrak{G} = 1$.

2) $X = \{o, 1, 2, 3\}$, $\mathfrak{G}$ fixes o ; on $\{1, 2, 3\}$, it is either $\mathfrak{S}_3$ or $\mathfrak{A}_3$.

3) $X = \{o\} \cup \mathbf{F}_5$, $\mathfrak{G}$ fixes o and is the group of affine linear transformations of $\mathbf{F}_5$.

Proof. Let $O \subset X$ be a $\mathfrak{G}$-orbit of cardinality $\leq d$. Pick $Y', Y \subset X$ with d elements such that $Y' \supset O$, $Y \cap O = \emptyset$. Then $gY' \supset O$, $gY \cap O = \emptyset$, $\forall\, g \in \mathfrak{G}$. Thus any subset of X of cardinality d either contains O or is disjoint with it. Let $o \in O$, $y \in Y$. The set $\{o\} \cup Y \backslash \{y\}$ has d elements and intersects O in $\{o\}$. So $O = \{o\}$.

Since $X \backslash \{o\}$ has $2d - 1$ elements and its subsets of cardinality d are permuted transitively by $\mathfrak{G}$, the previous lemma applies. □

Lemma 6.3. *Let $o \in X$, $\mathfrak{G}_o$ its stabilizer in $\mathfrak{G}$. If $\mathfrak{G}$ is transitive on X, $\mathfrak{G}_o < \mathfrak{H} < \mathfrak{G}$ for a group $\mathfrak{H}$, with $(\mathfrak{G} : \mathfrak{H})$ even, then either 1) or 2) holds :*

1) $X = \mathbf{Z}/4\mathbf{Z}$, $\mathfrak{G}$ consists of either all transformations

$$A_{a,b} : x \mapsto ax + b, \ x \in \mathbf{Z}/4\mathbf{Z}$$

$a \in (\mathbf{Z}/4\mathbf{Z})^\times$, $b \in \mathbf{Z}/4\mathbf{Z}$, or only $x \mapsto x+b$, $b \in \mathbf{Z}/4\mathbf{Z}$.

2) $X = \{1, \cdots, 6\}$, $\mathfrak{G}$ is either the normalizer in $\mathrm{Aut}(X)$ of a partition $X = \{a,b,c\} \cup \{u,v,w\}$, or a group $\mathfrak{Q}.\mathfrak{Alt}(\{a,b,c\}).\mathfrak{Alt}(\{u,v,w\})$, where $\mathfrak{Q}$ has generators in one of the following :

i) $(au)(bv)(cw)$

ii) $(aubv)(cw)$

iii) $(au)(bv)(cw), (ab)(uv)$

Proof. Let $(\mathfrak{G} : \mathfrak{H}) = 2r$. Note that

$$d = \frac{\mathrm{Card}(X)}{2} = \frac{(\mathfrak{G} : \mathfrak{H})}{2}(\mathfrak{H} : \mathfrak{G}_o) = r \ \mathrm{Card}(\mathfrak{H}.o).$$

If $\mathfrak{R} = \{g_1, \cdots, g_{2r}\} \subset \mathfrak{G}$ is a set of representatives for $\mathfrak{G}/\mathfrak{H}$, $Z := \{g_1, \cdots, g_r\}\mathfrak{H}.o$ has d elements.

As $\mathrm{Card}(\mathfrak{R}.o) \leq \mathrm{Card}(\mathfrak{R}) = 2r \leq d$, a set $Z' \supset \mathfrak{R}.o$ with d elements intersects all $g\mathfrak{H}.o$, $g \in \mathfrak{G}$.

Thus any subset of X of cardinality d either equals $\mathfrak{I}\mathfrak{H}.o$ for some $\mathfrak{I} \subset \mathfrak{R}$ of cardinality r, or intersects all $g\mathfrak{H}.o$, $g \in \mathfrak{G}$.

Necessarily, $r = 1$: if $r > 1$, $\{g_1, \cdots, g_r\}\mathfrak{H}.o \cup \{g_{r+1}.o\} \backslash \{g_1.o\}$ has d elements, is disjoint with $g_{2r}\mathfrak{H}.o$, but is not a $\mathfrak{I}\mathfrak{H}.o$, for any $\mathfrak{I} \subset \mathfrak{R}$.

So $\mathfrak{R} = \{g_1, g_2\}$, $\mathrm{Card}(\mathfrak{H}.o) = d$, $X = \mathfrak{H}.o \cup \tau\mathfrak{H}.o$, $\tau = g_1^{-1}g_2$, and the subsets of X of cardinality d distinct from $\mathfrak{H}.o$, $\tau\mathfrak{H}.o$ are permuted transitively by $\mathfrak{G}$.

Show $d \leq 3$: if $d > 3$, if $o' \in \mathfrak{H}.o\backslash\{o\}$, both

$$Y = \{o\} \cup \tau\mathfrak{H}.o\backslash\{\tau.o\} \ , \ Y' = \{o, o'\} \cup \tau\mathfrak{H}.o\backslash\{\tau.o, \tau.o'\}$$

are of cardinality d, different from $\mathfrak{H}.o$, $\tau\mathfrak{H}.o$, but $Y \neq gY'$, $\forall \ g \in \mathfrak{G}$, for $Y \cap \mathfrak{H}.o$ has 1 element, while $gY' \cap \mathfrak{H}.o$, as $Y' \cap g^{-1}\mathfrak{H}.o$, has either 2 or $d-2$ elements.

If $d = 2$, $\mathrm{Card}(X) = 4$, $\mathrm{Card}(\mathfrak{H}.o) = 2$, $\mathfrak{H} \leq \mathrm{Aut}(\mathfrak{H}.o) \times \mathrm{Aut}(\tau\mathfrak{H}.o)$, $\mathrm{Card}(\mathfrak{H}) = 4$ or 2, $\mathrm{Card}(\mathfrak{G}) = 8$ or 4.

If $\mathrm{Card}(\mathfrak{G}) = 8$, $\mathfrak{G}$ is a 2-Sylow subgroup of $\mathrm{Aut}(X) = \mathfrak{S}_4$, therefore is isomorphic to the group of transformations $A_{a,b} : x \mapsto ax + b$, $a \in (\mathbf{Z}/4\mathbf{Z})^\times$, $b \in \mathbf{Z}/4\mathbf{Z}$, on $X = \mathbf{Z}/4\mathbf{Z}$. The subgroup $\mathfrak{H}$ consists of those $A_{a,b} : x \mapsto ax + b$, where $b \equiv 0 \bmod 2$; it is the Klein group and permutes the 2-point subsets of X in 3 orbits.

If $\mathrm{Card}(\mathfrak{G}) = 4$, $\mathfrak{G}$ is of index 2 in a 2-Sylow subgroup of $\mathfrak{S}_4$, but cannot be a Klein group, thus must be the group of translations $x \mapsto x + b$, $b \in \mathbf{Z}/4\mathbf{Z}$, on $X = \mathbf{Z}/4\mathbf{Z}$. And $\mathfrak{H}$ consists of those $x \mapsto x + b$, where $b \equiv 0 \bmod 2$.

In either case, $\{0,2\}$, $\{1,3\}$ form one $\mathfrak{G}$-orbit, and $\{0,1\}$, $\{0,3\}$, $\{2,1\}$, $\{2,3\}$ form the other orbit, hence 1).

Consider $d = 3$, $\mathrm{Card}(X) = 6$. Evidently, $\mathfrak{G}$ is not contained in $\mathrm{Aut}(\mathfrak{H}.o) \times \mathrm{Aut}(\tau\mathfrak{H}.o)$. Let $\mathfrak{N}$ be the normalizer in $\mathrm{Aut}(X)$ of the partition $X = \mathfrak{H}.o \cup \tau\mathfrak{H}.o$; $\mathrm{Card}(\mathfrak{N}) = 72$. As the 3-point subsets of X distinct from $\mathfrak{H}.o$ and $\tau\mathfrak{H}.o$, 18 in number, are permuted transitively by $\mathfrak{G}$, $\mathrm{Card}(\mathfrak{G})$ is divisible by 18, $(\mathfrak{N} : \mathfrak{G}) = 1, 2$ or 4.

Write $X = \{1, \cdots, 6\}$, $\mathfrak{H}.o = \{1, 2, 3\}$, $\tau\mathfrak{H}.o = \{4, 5, 6\}$. Then $\mathfrak{G} = \mathfrak{P}\mathfrak{Q}$, where $\mathfrak{P} = \mathfrak{Alt}(\{1, 2, 3\}) \times \mathfrak{Alt}(\{4, 5, 6\})$, $\mathfrak{Q}$ is a 2-Sylow subgroup of $\mathfrak{G}$, of order $2, 4$ or 8.

i) If $\mathrm{Card}(\mathfrak{Q}) = 2$, i.e. $\mathfrak{Q} = \{1, \gamma\}$, γ is of order 2. If say $\gamma : 1 \mapsto 4$, $2 \mapsto 5$, $3 \mapsto 6$, then $\gamma = (14)(25)(36)$.

ii) Suppose $\mathfrak{Q}$ is cyclic of order 4 of generator γ, and $\gamma : 1 \mapsto 4$, $2 \mapsto 5$, $3 \mapsto 6$. As γ^2 is of order 2, normalizes $\{1, 2, 3\}$, it fixes a point, say 3. Then $\gamma^2(6) = \gamma^2(\gamma(3)) = \gamma(\gamma^2(3)) = \gamma(3) = 6$, so $\gamma = (1425)(36)$.

iii) Consider $\mathfrak{Q} = \{1, \alpha, \beta, \gamma\}$ of order 4, non cyclic, γ normalizing $\{1, 2, 3\}$. Then γ fixes a point, say 3. If $\beta : 1 \mapsto 4$, $2 \mapsto 5$, $3 \mapsto 6$, i.e. $\beta = (14)(25)(36)$, then $\alpha(3) = \alpha(\gamma(3)) = \beta(3) = 6$, and $\alpha = (15)(24)(36)$, $\gamma = (12)(45)$.

iv) If $\mathrm{Card}(\mathfrak{Q}) = 8$, $\mathfrak{G} = \mathfrak{N}$.

Observe that $\mathfrak{P}$ has 4 orbits on the 3-point subsets of X; and, one inspects that in all the cases i)–iv) $\mathfrak{G}$ permutes the 3-point subsets of X in 2 orbits, hence 2). □

Lemma 6.4. *Let $o \in X$, $\mathfrak{G}_o$ its stabilizer in $\mathfrak{G}$. If $\mathfrak{G}$ is transitive on X, $\mathfrak{G}_o < \mathfrak{H} < \mathfrak{G}$, with $(\mathfrak{G} : \mathfrak{H})$ odd, then $X = \{1, \cdots, 6\}$, $\mathfrak{G}$ is either the normalizer $\mathfrak{N}$ in $\mathrm{Aut}(X)$ of a partition $X = \{a, a'\} \cup \{b, b'\} \cup \{c, c'\}$, or the subgroup of $\mathfrak{N}$ generated by (aa'), (bb'), (cc'), $(abc)(a'b'c')$.*

Proof. Let $(\mathfrak{G} : \mathfrak{H}) = 2r + 1$, $r \geq 1$, $\mathfrak{R} = \{g_1, \cdots, g_{2r+1}\} \subset \mathfrak{G}$ a set of representatives for $\mathfrak{G}/\mathfrak{H}$. Since

$$d = \frac{\mathrm{Card}(X)}{2} = \frac{(\mathfrak{G} : \mathfrak{H})}{2}(\mathfrak{H} : \mathfrak{G}_o) = (r + \frac{1}{2})\ \mathrm{Card}(\mathfrak{H}.o),$$

$\mathrm{Card}(\mathfrak{H}.o)$ is even, $= 2f$, $f \geq 1$. Pick $B \subset g_{r+1}\mathfrak{H}.o \backslash \{g_{r+1}.o\}$ of cardinality f. Then $Y = \{g_1, \cdots, g_r\}\mathfrak{H}.o \cup B$ has d elements. As $\mathrm{Card}(\mathfrak{R}.o) \leq \mathrm{Card}(\mathfrak{R}) \leq d$, a set $Y' \supset \mathfrak{R}.o$ with d elements intersects all $g\mathfrak{H}.o$, $g \in \mathfrak{G}$. Hence any subset Z of X of cardinality d either intersects all $g\mathfrak{H}.o$, $g \in \mathfrak{G}$, or equals $\mathfrak{I}\mathfrak{H}.o \cup B'$, for some $\mathfrak{I} \subset \mathfrak{R}$ of cardinality r, some $B' \subset z\mathfrak{H}.o$ of cardinality f, $z \in \mathfrak{R} \backslash \mathfrak{I}$. In the latter case, Z intersects precisely $r + 1$ members of $\{g_1\mathfrak{H}.o, \cdots, g_{2r+1}\mathfrak{H}.o\}$.

Show $f = 1$: if $f > 1$, the set

$$\{g_1, \cdots, g_{r-1}\}\mathfrak{H}.o \cup (g_r\mathfrak{H}.o \backslash \{g_r.o\}) \cup (B \cup \{g_{r+1}.o\})$$

has d elements, is disjoint with $g_{2r+1}\mathfrak{H}.o$, but is not a $\mathfrak{I}\mathfrak{H}.o \cup B'$ for any $\mathfrak{I} \subset \mathfrak{R}$ of cardinality r, $B' \subset z\mathfrak{H}.o$ of cardinality f, $z \in \mathfrak{R}\backslash\mathfrak{I}$.

Thus $\mathrm{Card}(B) = f = 1$, $d = 2r + 1$.

Show $r = 1$: if $r > 1$, the set

$$\{g_1, \cdots, g_{r-1}\}\mathfrak{H}.o \cup (g_r\mathfrak{H}.o \backslash \{g_r.o\}) \cup \{g_{r+1}.o\} \cup \{g_{2r+1}.o\}$$

has d elements, is disjoint with $g_{r+2}\mathfrak{H}.o$, but intersects $r + 2$ members of $\{g_1\mathfrak{H}.o, \cdots, g_{2r+1}\mathfrak{H}.o\}$.

This gives $d = 2r + 1 = 3$, $\mathfrak{R} = \{g_1, g_2, g_3\}$, $\mathrm{Card}(\mathfrak{H}.o) = 2$, and X has 6 elements, 20 subsets of cardinality 3, among which 8 intersect all $g_j\mathfrak{H}.o$, $j \in \{1, 2, 3\}$. So $\mathfrak{G}$ has order divisible by 8 and by $20 - 8 = 12$, thus divisible by 24 ; it is either $\mathfrak{N}$, the normalizer in $\mathrm{Aut}(X)$ of the partition $X = g_1\mathfrak{H}.o \cup g_2\mathfrak{H}.o \cup g_3\mathfrak{H}.o$, or the subgroup of $\mathfrak{N}$ of index 2, generated by $\mathrm{Aut}(g_j\mathfrak{H}.o)$ and an element $\gamma \in \mathrm{Aut}(X)$ of order 3, which rotates $g_j\mathfrak{H}.o$, $j = 1, 2, 3$.

In either case, $\mathfrak{G}$ permutes the 3-point sets of X in 2 orbits, hence the lemma. □

Lemma 6.5. *Let $o \in X$, $\mathfrak{G}_o$ its stabilizer in $\mathfrak{G}$. If $\mathfrak{G}$ is transitive on X, and $\mathfrak{G}_o$ is a maximal subgroup of $\mathfrak{G}$, then $X = \mathbf{F}_8$, $\mathfrak{G}$ consists of either all affine semi-linear transformations*

$$A_{a,b,c} : x \mapsto ax^{2^c} + b, \ x \in \mathbf{F}_8,$$

$a \in \mathbf{F}_8^\times$, $b \in \mathbf{F}_8$, $c \in \mathbf{Z}/3\mathbf{Z}$, or only the affine linear transformations

$$A_{a,b} : x \mapsto ax + b, \ x \in \mathbf{F}_8,$$

$a \in \mathbf{F}_8^\times$, $b \in \mathbf{F}_8$.

Proof. One has $\mathfrak{G} = V\mathfrak{G}_o$, for a group V, where V is normal in $\mathfrak{G}$, simply transitive on X, isomorphic to a vector space over a prime field $\mathbf{F}_p$, and is a faithful irreducible representation of $\mathfrak{G}_o$. Identify V with X via the bijection $v \mapsto v.o$. If $f = \dim V$, $p^f = \mathrm{Card}(V) = \mathrm{Card}(X) = 2d$. So $p = 2$, $d = 2^{f-1}$. Clearly, $f > 1$.

Show $f > 2$: otherwise, $\mathfrak{G}_o$ being irreducible on V, cannot be a 2-group, thus is of order divisible by 3. So, $\mathfrak{G} = \mathfrak{S}_4$ or $\mathfrak{A}_4$. But both are transitive, rather than have 2 orbits, on the 2-point subsets of X.

Therefore, $d = 2^{f-1} \geq 4$.

A hyperplane H of V has $2^{f-1} = d$ elements. Given different hyperplanes H_1, H_2, the intersection $H_1 \cap H_2$ has dimension $f - 2$, cardinality

$2^{f-2} = d/2$, and $\mathrm{Card}(H_2\backslash H_1) = d/2$. For any $g \in \mathfrak{G}$, either gH or $V\backslash gH$ is a hyperplane. Consequently, $\mathrm{Card}(gH\backslash H) \in \{0, d, d/2\}$.

Fix $v \in V\backslash H$. The set $Y := \{v\} \cup H\backslash\{0\}$ has d elements. As $\mathrm{Card}(Y\backslash H) = 1 \notin \{0, d, d/2\}$, neither Y nor its complement is a hyperplane.

Hence the subsets of V of cardinality d are gH, and gY, $g \in \mathfrak{G}$.

Show $f = 3$: if $f \geq 4$, if $u \in H\backslash\{0\}$, the set

$$Z = \{v, u + v\} \cup H\backslash\{0, u\}$$

is of cardinality d, $\neq gH, gY$, because $\mathrm{Card}(gH\backslash H) \in \{0, d, d/2\}$, $\mathrm{Card}(gY\backslash H) = \mathrm{Card}(Y\backslash g^{-1}H) \in \{1, d-1, d/2, (d/2) \pm 1\}$, while $\mathrm{Card}(Z\backslash H) = 2 \neq 0, 1, d, d-1, d/2, (d/2) \pm 1$, as $d \geq 8$.

Now $\mathbf{P}(V) = \mathbf{P}^2$; it has 7 points rational over $\mathbf{F}_2$, that is, V has 7 hyperplanes. So 7 divides $\mathrm{Card}(\mathfrak{G})$ and $\mathrm{Card}(\mathfrak{G}_o)$. Once choosing an identification $V = \mathbf{F}_8$, a 7-Sylow subgroup of $\mathfrak{G}_o$ is the group of scalar multiplications $\sigma_a : x \mapsto ax$, $x \in \mathbf{F}_8$, $a \in \mathbf{F}_8^\times$.

Suppose $g \in \mathrm{GL}(V)$ normalizes $\{\sigma_a\}$. As $\det(T - g\sigma_a g^{-1}, V) = \det(T - \sigma_a, V) = (T-a)(T-a^2)(T-a^4)$, there exists a $c \in \mathbf{Z}/3\mathbf{Z}$ such that $g\sigma_a g^{-1} = \sigma_{F^c(a)} = F^c\sigma_a F^{-c}$, where $F : x \mapsto x^2$ is the Frobenius. It follows that $F^{-c}g$ commutes with $\{\sigma_a\}$, thus lies in $\{\sigma_a\}$. Hence the normalizer $\mathfrak{N}$ of $\{\sigma_a\}$ in $\mathrm{GL}(V)$ is the group of transformations $x \mapsto ax^{2^c}$, $a \in \mathbf{F}_8^\times$, $c \in \mathbf{Z}/3\mathbf{Z}$. Note that $\mathrm{Card}(\mathfrak{N}) = 21$.

Show $2 \nmid \mathrm{Card}(\mathfrak{G}_o)$: otherwise, $\mathfrak{G}_o$ being solvable, let $\mathfrak{H} \leq \mathfrak{G}_o$ be a Hall subgroup containing $\{\sigma_a\}$ and of order 7.2^j, $j \geq 1$. Necessarily, $j \leq 3$, because $\mathrm{Card}(\mathrm{GL}(V)) = 2^3.3.7$. As $\mathrm{Card}(\mathfrak{N}) = 21$, $\mathfrak{H}$ is not a subgroup of $\mathfrak{N}$, that is, $\{\sigma_a\}$ is not normal in $\mathfrak{H}$, so $j \neq 1, 2$. If $j = 3$, $\mathfrak{H}$ has a unique 2-Sylow subgroup $\mathfrak{Q}$, for the number of 7-Sylow subgroups of $\mathfrak{H}$ is $\equiv 1 \bmod 7$, i.e. 8. Then since $\mathfrak{Q}$ is 2-Sylow in $\mathrm{GL}(V)$, the center of $\mathfrak{Q}$ is of order 2, normalized by $\{\sigma_a\}$, thus centralized by $\{\sigma_a\}$, therefore contained in $\mathfrak{N}$. This is absurd.

As $\mathrm{Card}(\mathfrak{G}_o) = 7$ or 21, $\{\sigma_a\}$ is normal in $\mathfrak{G}_o$, i.e. $\mathfrak{G}_o \leq \mathfrak{N}$, and $\mathfrak{G}$ may be $V\mathfrak{N}$, the group of affine semi-linear transformations

$$A_{a,b,c} : x \mapsto ax^{2^c} + b,\ x \in \mathbf{F}_8,$$

$a \in \mathbf{F}_8^\times$, $b \in \mathbf{F}_8$, $c \in \mathbf{Z}/3\mathbf{Z}$, or its subgroup $V\{\sigma_a\}$ consisting of the affine linear transformations

$$A_{a,b} : x \mapsto ax + b,\ x \in \mathbf{F}_8,$$

$a \in \mathbf{F}_8^\times$, $b \in \mathbf{F}_8$.

In $\mathbf{F}_8$, there are 70 subsets of cardinality 4. So both groups have > 1 orbits on these subsets. The 7 hyperplanes and their complements evidently form one orbit under either group. Given a Y in the rest $70-14=56$ subsets of cardinality 4, if $\mathfrak{S}$ denotes the stabilizer of Y in $V\{\sigma_a\}$, then $\mathfrak{S} \leq \mathrm{Aut}(Y) = \mathfrak{S}_4$, in particular, $7 \nmid \mathrm{Card}(\mathfrak{S})$, so $\mathfrak{S}$ is contained in the group of translations, thus $\mathfrak{S} = 1$, by the choice of Y, whence the orbit $V\{\sigma_a\}.Y$ consists of 56 members. This concludes the proof. □

Summarizing (6.2)–(6.5), one obtains

Proposition 6.6. *Let d be an integer ≥ 1, X a set with $2d$ elements, $\mathfrak{G} \leq \mathrm{Aut}(X)$ a solvable subgroup permuting the subsets of X of cardinality d in 2 orbits. Then $X, \mathfrak{G}$ are classified as*

1) $X = \{o, 1\}$, $\mathfrak{G} = 1$.

2) $X = \{o, 1, 2, 3\}$, $\mathfrak{G}$ fixes o ; on $\{1, 2, 3\}$, it is $\mathfrak{S}_3$ or $\mathfrak{A}_3$.

3) $X = \{o\} \cup \mathbf{F}_5$, $\mathfrak{G}$ fixes o and is the group of affine linear transformations of $\mathbf{F}_5$.

4) $X = \mathbf{Z}/4\mathbf{Z}$, $\mathfrak{G}$ consists of either all transformations

$$A_{a,b} : x \mapsto ax + b, \ x \in \mathbf{Z}/4\mathbf{Z},$$

$a \in (\mathbf{Z}/4\mathbf{Z})^\times$, $b \in \mathbf{Z}/4\mathbf{Z}$, or only $x \mapsto x + b$, $b \in \mathbf{Z}/4\mathbf{Z}$.

5) $X = \{1, \cdots, 6\}$, $\mathfrak{G}$ is either the normalizer in $\mathrm{Aut}(X)$ of a partition $X = \{a, b, c\} \cup \{u, v, w\}$, or a group $\mathfrak{Q}.\mathfrak{Alt}(\{a, b, c\}).\mathfrak{Alt}(\{u, v, w\})$, where $\mathfrak{Q}$ has generators in i), or ii) or iii) :

i) $(au)(bv)(cw)$

ii) $(aubv)(cw)$

iii) $(au)(bv)(cw), (ab)(uv)$.

6) $X = \{1, \cdots, 6\}$, $\mathfrak{G}$ is either the normalizer $\mathfrak{N}$ in $\mathrm{Aut}(X)$ of a partition $X = \{a, a'\} \cup \{b, b'\} \cup \{c, c'\}$, or the subgroup of $\mathfrak{N}$ generated by (aa'), (bb'), (cc'), $(abc)(a'b'c')$.

7) $X = \mathbf{F}_8$, $\mathfrak{G}$ consists of either all affine semi-linear transformations

$$A_{a,b,c} : x \mapsto ax^{2^c} + b, \ x \in \mathbf{F}_8,$$

$a \in \mathbf{F}_8^\times$, $b \in \mathbf{F}_8$, $c \in \mathbf{Z}/3\mathbf{Z}$, or only the affine linear transformations

$$A_{a,b} : x \mapsto ax + b, \ x \in \mathbf{F}_8,$$

$a \in \mathbf{F}_8^\times$, $b \in \mathbf{F}_8$.

Lemma 6.7. *Let d be an integer ≥ 1, X a set with $2d$ elements, $\mathfrak{G}$ a solvable subgroup of $\mathrm{Aut}(X)$ permuting transitively the subsets of X of cardinality d. Then $X, \mathfrak{G}$ are*

1) $X = \{1, 2\}$, $\mathfrak{G} = \mathfrak{S}_2$.

2) $X = \{1, 2, 3, 4\}$, $\mathfrak{G} = \mathfrak{S}_4$ or $\mathfrak{A}_4$.

Proof. Let $o \in X$ be a point, $\mathfrak{G}_o$ its stabilizer in $\mathfrak{G}$. As usual, $\mathfrak{G} = V\mathfrak{G}_o$, V normal in $\mathfrak{G}$, simply transitive on X, isomorphic to a vector space over a prime field $\mathbf{F}_p$, and is a faithful irreducible representation of $\mathfrak{G}_o$. Write $f = \dim V$. Then $p^f = \mathrm{Card}(V) = \mathrm{Card}(X) = 2d$, so $p = 2$, $d = 2^{f-1}$.

Identify V with X through the bijection $v \mapsto v.o$. Every subset of V of cardinality d is some gH, $g \in \mathfrak{G}$, where H is a fixed hyperplane in V. So $f \leq 2$, for otherwise, neither $Y := \{v\} \cup H \backslash \{0\}$ nor its complement is a hyperplane, if a vector v is chosen in the complement of H.

If $f = 1$, $X = \{1, 2\}$, on which $\mathfrak{G}$ is transitive, so $\mathfrak{G} = \mathfrak{S}_2$.

If $f = 2$, as $\mathfrak{G}_o$ is irreducible on V, it is not a 2-group, thus has order divisible by 3. Hence, $\mathfrak{G} = \mathfrak{S}_4$ or $\mathfrak{A}_4$. Both do permute transitively the 2-point subsets of X. □

Proposition 6.8. *Let d be an integer ≥ 2, X a set with $2d$ elements, $\mathfrak{G} \leq \{1, -1\} \times \mathrm{Aut}(X)$ a solvable subgroup permuting transitively the subsets of X of cardinality d, $\mathfrak{G} \not\leq \mathrm{Aut}(X)$. Here -1 sends any Y of cardinality d to $X \backslash Y$. Then $X, \mathfrak{G}$ are*

1) $X = \{o, a, b, c\}$, $\mathfrak{G} = \{1, -1\}\mathfrak{S}_4$, $\{1, -1\}\mathfrak{A}_4$, $\{1, -1.(oa)\}\mathfrak{A}_4$, $\{1, -1\}\mathrm{Aut}(\{a, b, c\})$, $\{1, -1\}\mathfrak{Alt}(\{a, b, c\})$, $\{1, -1.(oa)\}\mathfrak{Alt}(\{a, b, c\})$.

2) $X = \{o\} \cup \mathbf{F}_5$, $\mathfrak{G} = \{1, -1\} \times \mathfrak{H}$, where $\mathfrak{H}$ fixes o and is the group of affine linear transformations of $\mathbf{F}_5$.

Proof. The subgroup $\mathfrak{H} := \mathfrak{G} \cap \mathrm{Aut}(X)$ is of index 2 in $\mathfrak{G}$. Let Y be a subset of X of cardinality d, $\mathfrak{S}$ be its normalizer in $\mathfrak{G}$. If $\mathfrak{S} \not\leq \mathfrak{H}$, $\mathfrak{H}$ is transitive on $\mathfrak{G}/\mathfrak{S}$. If $\mathfrak{S} \leq \mathfrak{H}$, $\mathfrak{H}/\mathfrak{S} \subset \mathfrak{G}/\mathfrak{S}$ exhausts half among all subsets of X of cardinality d ; in particular, $\mathfrak{H}$ has 2 orbits on $\mathfrak{G}/\mathfrak{S}$.

If $\mathfrak{H}$ is transitive on $\mathfrak{G}/\mathfrak{S}$, then $\mathrm{Card}(X) = 4$, $\mathfrak{H} = \mathfrak{S}_4$ or $\mathfrak{A}_4$ (6.7). Accordingly, $\mathfrak{G}$ is either $\{1, -1\}\mathfrak{S}_4$ or a subgroup of $\{1, -1\}\mathfrak{S}_4$ of index 2 containing $\mathfrak{A}_4$, i.e. $\{1, -1\}\mathfrak{A}_4$ or $\{1, -1.(ab)\}\mathfrak{A}_4$, for some (ab).

If $\mathfrak{H}$ permutes $\mathfrak{G}/\mathfrak{S}$ in 2 orbits of the same size, then by the proof of (6.6), i) or ii) holds :

i) $X = \{o, 1, 2, 3\}$, $\mathfrak{H} = \mathrm{Aut}(\{1, 2, 3\})$ or $\mathfrak{Alt}(\{1, 2, 3\})$.

ii) $X = \{o\} \cup \mathbf{F}_5$, $\mathfrak{H}$ fixes o and is the group of affine linear transformations of $\mathbf{F}_5$.

Let $\mathfrak{N}$ denote the normalizer of $\mathfrak{H}$ in $\{1, -1\}\mathrm{Aut}(X)$. Clearly, $\mathfrak{G} \leq \mathfrak{N}$.

In case i), both $\mathrm{Aut}(\{1, 2, 3\})$ and $\mathfrak{Alt}(\{1, 2, 3\})$ have normalizer equal to $\{1, -1\}\mathrm{Aut}(X) = \mathfrak{N}$. If $\mathfrak{H} = \mathrm{Aut}(\{1, 2, 3\})$, $\mathfrak{G} = \mathfrak{N}$.

If $\mathfrak{H} = \mathfrak{Alt}(\{1,2,3\})$, $(\mathfrak{N} : \mathfrak{G}) = 2$, $\mathfrak{G} = \{1,-1\}\mathfrak{Alt}(\{1,2,3\})$ or $\{1,-1.(oa)\}\mathfrak{Alt}(\{1,2,3\})$, for some $a \in \{1,2,3\}$.

In case ii), $\mathfrak{N} = \{1,-1\} \times \mathfrak{H}$: if $g \in \mathfrak{N} \cap \mathrm{Aut}(X)$, $\mathfrak{H}g.o = g\mathfrak{H}.o = g.o$. So $g.o = o$, and g preserves $\mathbf{F}_5$. Let

$$A : x \mapsto (g(1) - g(0))x + g(0),\ x \in \mathbf{F}_5$$

Then $h := g^{-1}A$ fixes $o, 0, 1$, normalizes $\{T_b : x \mapsto x + b\}$, the unique 5-Sylow subgroup of $\mathfrak{H}$.

As $hT_1h^{-1}(0) = 1 = T_1(0)$, $hT_1h^{-1} = T_1$, that is, h commutes with $\{T_b\}$, therefore $= 1$, for $h(b) = hT_b(0) = T_bh(0) = b$, $\forall\ b \in \mathbf{F}_5$. One finds that $g = A \in \mathfrak{H}$. Finally, $\mathfrak{G}$ can only be $\mathfrak{N}$. □

Proposition 6.9. *Let S, η, s be as in §4. Any $({}^2A_3, \alpha_2)$ over η is elliptic. If $n > 5$, $({}^2A_n, \alpha_{\frac{n+1}{2}})$ is not elliptic.*

Proof. That $({}^2A_n, \alpha_{\frac{n+1}{2}})$, n odd > 5, is not elliptic follows immediately from (3.1), 8), and (6.8).

For any pair $({}^2A_3, \alpha_2)$ over η, then in the notations of (6.8), 1), the group $\{1,-1\}\mathfrak{Alt}(\{a,b,c\}) = \mathbf{Z}/6\mathbf{Z}$ is clearly realizable as a quotient of $\pi_1(\eta, \overline{\eta})$ lifting the given index, that is to say, $({}^2A_3, \alpha_2)$ is elliptic over η, (3.1), 8). □

Proposition 6.10. *Let S, η, s be as in §4,* $\mathrm{char}(s) = \ell$. *If $\ell = 5$, any $({}^2A_5, \alpha_3)$ over η is elliptic. When $(\ell, 5) = 1$, a pair $({}^2A_5, \alpha_3)$ over η is elliptic if and only if ${}^2A_5$ is ramified over S, and* $\mathrm{Card}(k(s))$ *mod 5 generates $\mathbf{F}_5^\times$.*

Proof. By (3.1), 8), and (6.8), 2), a pair $({}^2A_5, \alpha_3)$ over η is elliptic if and only if there exists a surjection

$$\rho = (\rho_1, \rho_2) : \pi_1(\eta, \overline{\eta}) \to \{1,-1\} \times \mathfrak{H} = \mathfrak{G},$$

whose first component is the index of ${}^2A_5$, where $\mathfrak{H}$ denotes the group of affine linear transformations of $\mathbf{F}_5$.

Note that $\mathfrak{H}$ is a quotient of $\pi_1(\eta, \overline{\eta})$ if and only if either $\ell = 5$ (4.1), or $(\ell, 5) = 1$, $\mathrm{Card}(k(s))$ mod 5 generates $\mathbf{F}_5^\times$, (4.2), 2).

Let ${}^2A_5' \to \eta$ correspond to the index of ${}^2A_5$.

Suppose first ${}^2A_5'$ be unramified over S.

If $\rho = (\rho_1, \rho_2)$ exists, ρ_2 has to be totally ramified over S, so $\ell = 5$. When $\ell = 5$, choosing a uniformizer $\pi \in \Gamma(\mathcal{O}_S)$, then

$${}^2A_5' \times_\eta \eta[z,x]/(z^4 - \pi, x^5 - x - z^{-1})$$

is Galois over η of group $\mathfrak{G}$.

Next, assume ${}^2A_5'$ is ramified over S.

If $\ell = 5$, letting $\pi \in \Gamma(\mathcal{O}_S)$ be a uniformizer, $\eta' \to \eta$ be connected, unramified over S of degree 4, S' the normalization of S in η, $s' \in S'$ the closed point, $\zeta \in \mathrm{Gal}(\eta'/\eta)$ a generator, and $u' \in \Gamma(\mathcal{O}_{S'})^\times$ such that the images of $u', \zeta(u'), \zeta^2(u'), \zeta^3(u')$ in $k(s')$ form a normal base over $k(s)$, then

$$^2A'_5 \times_\eta \eta'[x_1, \cdots, x_4]/(x_1^5 - x_1 - \zeta(u')\pi^{-1}, \cdots, x_4^5 - x_4 - \zeta^4(u')\pi^{-1})$$

is Galois over η of group $\mathfrak{G}$.

If $(\ell, 5) = 1$, and $\mathrm{Card}(k(s))$ mod 5 generates $\mathbf{F}_5^\times$, then $^2A'_5 \times_\eta \eta'$ is Galois over η of group $\mathfrak{G}$, where $\eta' \to \eta$ is tame along s, Galois, of Galois group $\mathfrak{H}$, cf. (4.2), 2). □

7. Type B

Let S, η, s be as in §4.

Let n be an integer ≥ 3, $e_1, \cdots, e_n$ the standard base of $\mathbf{Z}^n$, and $\mathfrak{W}$ the subgroup of $\mathrm{GL}_n(\mathbf{Z})$ generated by the diagonal matrices and monomial matrices.

Proposition 7.1. *If* $\mathrm{char}(s) = 2$, *(B_n, α_n) is elliptic over η.*

Proof. It is because the group generated by the diagonal matrices and the element $\zeta : e_1 \mapsto e_2, \cdots, e_n \mapsto e_1$, permutes transitively the vectors $\pm e_1 \pm \cdots \pm e_n$, and is a quotient of $\pi_1(\eta, \overline{\eta})$, (4.1), (3.1), 2). □

Proposition 7.2. *The pair (B_3, α_3) is elliptic over η.*

Proof. The elements a, b of $\mathrm{GL}_3(\mathbf{Z})$,

$$\begin{cases} a : e_1 \mapsto e_1,\ e_2 \mapsto e_3,\ e_3 \mapsto -e_2 \\ b : e_1 \mapsto -e_1,\ e_2 \mapsto e_2,\ e_3 \mapsto e_3 \end{cases}$$

satisfy the relations

$$a^4 = 1,\ b^2 = 1,\ ab = ba.$$

The group $\langle a, b \rangle = \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is simply transitive on $\{\pm e_1 \pm e_2 \pm e_3\}$, and is a quotient of $\pi_1(\eta, \overline{\eta})$. So (B_3, α_3) is elliptic over η, (3.1), 2). □

Proposition 7.3. *If* $\mathrm{char}(s) > 2$, *(B_4, α_4) is elliptic over η.*

Proof. Define $a, b, c, d \in \mathrm{GL}_4(\mathbf{Z})$ by

$$\begin{cases} a : e_1 \mapsto e_2,\ e_2 \mapsto -e_1,\ e_3 \mapsto e_3,\ e_4 \mapsto e_4 \\ b : e_1 \mapsto e_1,\ e_2 \mapsto e_2,\ e_3 \mapsto e_4,\ e_4 \mapsto -e_3 \end{cases}$$

$$\begin{cases} c : e_1 \mapsto e_2,\ e_2 \mapsto e_3,\ e_3 \mapsto e_4,\ e_4 \mapsto -e_1 \\ d : e_1 \mapsto e_3,\ e_2 \mapsto -e_4,\ e_3 \mapsto -e_1,\ e_4 \mapsto e_2 \end{cases}$$

They satisfy the relations

$$a^4 = b^4 = 1,\ ab = ba,\ c^8 = 1,\ d^4 = 1,\ cdc^{-1} = d^{-1}.$$

The group $\langle c, d\rangle$ is quaternion of order 16, and $\langle a, b\rangle$ is isomorphic to $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Both are simply transitive on $\{\pm e_1 \pm e_2 \pm e_3 \pm e_4\}$.

If $\mathrm{Card}(k(s)) \equiv 1 \bmod 4$ (resp. $\mathrm{Card}(k(s)) \equiv -1 \bmod 4$), $\langle a, b\rangle$ (resp. $\langle c, d\rangle$) is a quotient of $\pi_1^t(\eta, \overline{\eta})$. So (B_4, α_4) is elliptic over η, when $\mathrm{char}(s)$ is odd. □

Proposition 7.4. *If* $\mathrm{char}(s) > 2$, (B_5, α_5) *is not elliptic over* η.

Proof. Assume (B_5, α_5) is elliptic, and $\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{W}$ is a representation whose monodromy is transitive on $\{\pm e_1 \pm \cdots \pm e_5\}$. Extending the base η if necessary, suppose the monodromy $\mathfrak{G}$ is a 2-group, in particular tame, with generators σ, τ, $\sigma\tau\sigma^{-1} = \tau^q$, $q = \mathrm{Card}(k(s))$. The order $\mathrm{Card}(\mathfrak{G})$ is divisible by 32.

Since $\mathrm{GL}_5(\mathbf{Z})$ contains no element of order 16, $\tau^8 = \sigma^8 = 1$.

For any $q \equiv 1, 3, 5$ or $7 \bmod 8$, $\sigma^2\tau\sigma^{-2} = \tau^{q^2} = \tau$, i.e. σ^2 commutes with τ.

If τ is of order 8, its characteristic polynomial is $(T^4 + 1)(T - 1)$ or $(T^4 + 1)(T + 1)$. Some vector in $\{e_1, \cdots, e_5\}$ is an eigenvector of τ, say $\tau(e_5) \in \{e_5, -e_5\}$. Then $\langle\tau\rangle$ normalizes and is simply transitive on $\{\pm e_1, \cdots, \pm e_4\}$. The equation $\sigma\tau\sigma^{-1} = \tau^q$ gives

$$\sigma(e_5) = \pm\sigma\tau(e_5) = \pm\tau^q\sigma(e_5).$$

So $\sigma(e_5) \in \{e_5, -e_5\}$, σ normalizes $\{\pm e_1, \cdots, \pm e_4\}$. Put

$$V = \mathbf{Z}e_1 + \mathbf{Z}e_2 + \mathbf{Z}e_3 + \mathbf{Z}e_4.$$

On V, $\sigma^2|V$, being commutative with $\tau|V$, equals some power of $\tau|V$, that is, $\sigma^2|V = \tau^i|V$, $i = 0, 2, 4$ or 6. For this i, as $\sigma^2(e_5) = \tau^i(e_5) = e_5$, one finds that $\sigma^2 = \tau^i$. But then $\mathfrak{G} = \langle\tau\rangle \cup \langle\tau\rangle\sigma$ is of order ≤ 16.

If $\tau^4 = 1$, σ is of order 8, and $\sigma\tau\sigma^{-1} = \tau$ or τ^{-1}. In either case, τ^2 commutes with σ.

If the characteristic polynomial of τ is $(T^2 + 1)^2(T \pm 1)$, with say $\tau(e_5) \in \{e_5, -e_5\}$. Note that then

$$\sigma(e_5) = \pm\sigma\tau(e_5) = \pm\tau^q\sigma(e_5), \quad q \equiv 1, -1 \bmod 4.$$

Therefore, σ normalizes $\{e_5, -e_5\}$, also normalizes $\{\pm e_1, \cdots, \pm e_4\}$. Similarly as above, $\tau^2 = \sigma^i$, $i \in \{0, 4\}$. But $\mathfrak{G} = \langle\sigma\rangle \cup \tau\langle\sigma\rangle \cup \tau^{-1}\langle\sigma\rangle$ has order ≤ 24.

If the characteristic polynomial of τ is $(T^2 + 1)(T + 1)^i(T - 1)^{3-i}$, $i \in \{0, 1, 2, 3\}$, with say $\tau(e_3) = \pm e_3$, $\tau(e_4) = \pm e_4$, $\tau(e_5) = \pm e_5$. Then

τ normalizes $\{\pm e_1, \pm e_2\}$. The equation $\sigma\tau\sigma^{-1} = \tau^q$ implies that σ normalizes $\{\pm e_3, \pm e_4, \pm e_5\}$, thus normalizes $\{\pm e_1, \pm e_2\}$. But then σ cannot have order 8. □

Proposition 7.5. *If* $\mathrm{char}(s) > 2$*,* $n \geq 6$*, then* (B_n, α_n) *is not elliptic over* η*.*

Proof. Assume (B_n, α_n) is elliptic, and $\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{W}$ is a representation with monodromy permuting transitively the vectors $\pm e_1 \pm \cdots \pm e_n$. Extend the base η so that the monodromy $\mathfrak{G}$ is a 2-group ; it is of order divisible by 2^n.

Write $\mathfrak{D}$ for the group of diagonal matrices in $\mathfrak{W}$. Let $\mathfrak{P}$ be the image of $\mathfrak{G}$ in $\mathfrak{S}_n = \mathfrak{W}/\mathfrak{D}$. The group $\mathfrak{D} \cap \mathfrak{G}$, being a sub-quotient of $\pi_1(\eta, \overline{\eta})$, has order ≤ 4. Hence, $\mathrm{Card}(\mathfrak{P})$ is divisible by 2^{n-2}.

Note that $\mathrm{ord}_2(n!) \leq n - 1$; the equality holds if and only if n is a power of 2.

Hence, if n is not a power of 2, $\mathfrak{P}$ is a 2-Sylow subgroup of $\mathfrak{S}_n$, so contains a conjugate of $\langle (12), (34), (56) \rangle$. But $\langle (12), (34), (56) \rangle$ cannot be a sub-quotient of $\pi_1(\eta, \overline{\eta})$.

If n is a power of 2, thus $n \geq 8$, $\mathfrak{P}$ is of index ≤ 2 in a 2-Sylow subgroup of $\mathfrak{S}_n$. So a conjugate of $\langle (12), (34), \cdots, (n-1, n) \rangle$, say $\mathfrak{Q}$, satisfies $(\mathfrak{Q} : \mathfrak{Q} \cap \mathfrak{P}) \leq 2$. But $\mathfrak{Q} \cap \mathfrak{P}$, being an elementary 2-group of order ≥ 8, cannot be a sub-quotient of $\pi_1(\eta, \overline{\eta})$ either. □

8. Type C

Proposition 8.1. *Let* η *be the spectrum of a completely discretely valued field of characteristic zero of finite residue field. For any integer* $n \geq 1$*,* (C_n, α_1) *is elliptic over* η*.*

Proof. The subgroup $\langle \tau\zeta \rangle$ of $\mathrm{GL}_n(\mathbf{Z})$, where $\zeta : e_1 \mapsto e_2, \cdots, e_n \mapsto e_1$, and $\tau : e_1 \mapsto -e_1$, $e_i \mapsto e_i$, $\forall\ i > 1$, is simply transitive on the set of vectors $\{e_1, \cdots, e_n, -e_1, \cdots, -e_n\}$.

As $\mathbf{Z}/2n\mathbf{Z} = \langle \tau\zeta \rangle$ is a quotient of $\pi_1(\eta, \overline{\eta})$, (C_n, α_1) is elliptic over η, (3.2), 3). □

9. Type D

Let S, η, s be as in §4.

Let n be an integer ≥ 3, $e_1, \cdots, e_n$ the standard base of $\mathbf{Z}^n$, $\mathfrak{W}_1$ the subgroup of $\mathrm{GL}_n(\mathbf{Z})$ generated by the diagonal matrices $\mathfrak{D}_1$ of determinant 1, and the monomial matrices $\mathfrak{M}$.

By conjugation, $\mathfrak{W}_1$ acts on $\mathfrak{D}_1$, $m : \mathfrak{W}_1 \to \mathrm{Aut}(\mathfrak{D}_1)$. This action gives the canonical split exact sequence

$$1 \to \mathfrak{D}_1 \to \mathfrak{W}_1 \xrightarrow{m} \mathfrak{M} \to 1.$$

Lemma 9.1. *A group of monomial matrices is normalized by a diagonal matrix δ if and only if it is centralized by δ.*

Proof. Let such a group of monomial matrices be $\mathfrak{H}$. For any $h \in \mathfrak{H}$, the element $\delta h \delta^{-1} h^{-1}$ is at the same time diagonal and monomial, so $\delta h \delta^{-1} h^{-1} = 1$, δ commutes with $\mathfrak{H}$. □

Lemma 9.2. *Any subgroup $\mathfrak{H}$ of $\mathfrak{W}_1$ of odd order is conjugate to $m(\mathfrak{H})$ by an element of $\mathfrak{D}_1$.*

Proof. Write any element of $\mathfrak{H}$ as

$$h = \delta(h)m(h), \quad \delta(h) \in \mathfrak{D}_1,\ m(h) \in \mathfrak{M}.$$

The function $h \mapsto \delta(h)$ is a cocycle of $\mathfrak{H}$ with values in $\mathfrak{D}_1$:

$$\delta(gh) = \delta(g)m(g)\delta(h)m(g)^{-1},\ \forall\ g, h \in \mathfrak{H}$$

hence, as $H^1(\mathfrak{H}, \mathfrak{D}_1) = 0$, is a coboundary : $\exists\ \delta \in \mathfrak{D}_1$, $\forall\ h \in \mathfrak{H}$,

$$\delta(h) = \delta m(h) \delta m(h)^{-1}.$$

For any $h \in \mathfrak{H}$,

$$h = \delta(h)m(h) = \delta m(h)\delta m(h)^{-1} m(h) = \delta m(h) \delta^{-1}.$$

So $\mathfrak{H} = \delta m(\mathfrak{H})\delta^{-1}$. □

Proposition 9.3. *If n is even, (D_n, α_1) is elliptic over η. If* $\mathrm{char}(s) = 2$*, (D_n, α_1), (D_n, α_{n-1}), (D_n, α_n) are elliptic over η. The pairs (D_4, α_3), (D_4, α_4) are elliptic over η.*

Proof. Let $\zeta : e_1 \mapsto e_2, \cdots, e_n \mapsto e_1$.

If n is even, $\langle -1, \zeta \rangle = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ lies in $\mathfrak{W}_1$, is a quotient of $\pi_1(\eta, \overline{\eta})$, and permutes transitively the vectors

$$e_1, \cdots, e_n, -e_1, \cdots, -e_n.$$

So, for n even, (D_n, α_1) is elliptic over η, (3.1), 4). In particular, (D_4, α_1), thus (D_4, α_i), $i = 3, 4$, are elliptic.

The group $\mathfrak{D}_1\langle\zeta\rangle$ is transitive on $\{\pm e_1, \cdots, \pm e_n\}$, on

$$\{s_1 e_1 + \cdots + s_n e_n,\ s_i \in \{1, -1\},\ s_1 \cdots s_n = -1\},$$

and on

$$\{s_1 e_1 + \cdots + s_n e_n,\ s_i \in \{1, -1\},\ s_1 \cdots s_n = 1\}.$$

If $\mathrm{char}(s) = 2$, $\mathfrak{D}_1\langle\zeta\rangle$ is also a quotient of $\pi_1(\eta,\overline{\eta})$: Let $\eta' \to \eta$ be connected, unramified over S of degree n, let S' be the normalization of S in η, $s' \in S'$ the closed point, $\pi \in \Gamma(\mathcal{O}_S)$ a uniformizer, $\zeta \in \mathrm{Gal}(\eta'/\eta)$ a generator, and $u' \in \Gamma(\mathcal{O}_{S'})^\times$ such that the images of $u', \zeta(u'), \cdots, \zeta^{n-1}(u')$ in $k(s')$ are a normal base over $k(s)$. If $b' := 1 + u'\pi$, then

$$\eta'[z_1, \cdots, z_n]/(z_1^2 - \frac{\zeta(b')}{b'},\ \cdots,\ z_{n-1}^2 - \frac{\zeta^{n-1}(b')}{\zeta^{n-2}(b')},\ z_n^2 - \frac{b'}{\zeta^{n-1}(b')})$$

is Galois over η of Galois group $\mathfrak{D}_1\langle\zeta\rangle$.

Hence, if $\mathrm{char}(s) = 2$, (D_n, α_1), (D_n, α_{n-1}), (D_n, α_n) are elliptic over η, (3.1), 4), 5). □

Proposition 9.4. *Suppose* $\mathrm{char}(s) > 2$. *For any odd integer* $n \geq 5$, (D_n, α_1) *is not elliptic over* η.

Proof. It suffices to show that for any odd integer $n \geq 5$ and for $n = 3$, no representation of $\pi_1(\eta,\overline{\eta})$ in $\mathfrak{W}_1$ has image transitive on $\{\pm e_1, \cdots, \pm e_n\}$, (3.1), 4).

Assume the contrary, and let n be the smallest odd integer ≥ 3 such that there exists a representation $\rho : \pi_1(\eta,\overline{\eta}) \to \mathfrak{W}_1$ whose image $\mathfrak{G}$ acts transitively on $\{\pm e_1, \cdots, \pm e_n\}$.

The inertia subgroup $\mathfrak{R}$ of $\mathfrak{G}$ is a semi-direct product $\mathfrak{S}\langle\tau\rangle$, where τ is of order a power of 2, $\mathfrak{S}$ is characteristic in $\mathfrak{R}$, of odd order, and contains the wild inertia subgroup of $\mathfrak{G}$.

Pick a 2-Sylow subgroup $\mathfrak{Q}$ of $\mathfrak{G}$ containing τ, and a Hall subgroup $\mathfrak{H}$ containing $\mathfrak{S}$, with $\mathrm{Card}(\mathfrak{G}) = \mathrm{Card}(\mathfrak{H})\mathrm{Card}(\mathfrak{Q})$.

By (9.2), for some $\delta \in \mathfrak{D}_1$, $\delta\mathfrak{H}\delta^{-1}$ is monomial. Changing ρ to $\mathrm{int}(\delta) \circ \rho$, assume $\mathfrak{H}$ is monomial. Therefore $\mathfrak{H}$, a priori $\mathfrak{S}$, normalizes $\{e_1, \cdots, e_n\}$.

Let the $\mathfrak{S}$-orbits in $\{e_1, \cdots, e_n\}$ be $O_1, \cdots, O_d$; the orbits have the same cardinality, since $\mathfrak{S}$ is normal in $\mathfrak{G}$.

Thus $n = d.\mathrm{Card}(O_i)$, and $d, \mathrm{Card}(O_i)$ are odd.

Given any $g = \delta(g)m(g) \in \mathfrak{G}$, with $\delta(g) \in \mathfrak{D}_1$, $m(g) \in \mathfrak{M}$, the equality $g\mathfrak{S}g^{-1} = \mathfrak{S}$ means

$$\delta(g)\mathfrak{S}\delta(g)^{-1} = m(g)\mathfrak{S}m(g)^{-1} = \mathfrak{S}.$$

By (9.1), $\delta(g)$ centralizes $\mathfrak{S}$; on each O_i, $i = 1, \cdots, d$, $\delta(g) = \pm 1$. And $m(g)$ permutes the orbits O_i.

Considering $O_1, \cdots, O_d$ as the standard base of $\mathbf{Z}^d$, the image of $\mathfrak{G}$ in $\mathrm{GL}_d(\mathbf{Z})$ lies in the group generated by the diagonal matrices of determinant 1 and monomial matrices.

So, by our choice of n, $d = 1$ or n.

If $d = 1$, $\mathfrak{S}$ is transitive on $\{e_1, \cdots, e_n\}$. For any $g \in \mathfrak{G}$, either g or $-g$ is monomial. As $-1 \notin \mathfrak{W}_1$, $\mathfrak{G}$ is monomial. But then $\mathfrak{G}$ cannot be transitive on $\{\pm e_1, \cdots, \pm e_n\}$.

Next, consider $d = n$. Then $\mathfrak{S} = 1$, $\mathfrak{G}$ is tame, $\mathfrak{R} = \langle \tau \rangle$, $\mathfrak{Q}$ is normal in $\mathfrak{G}$, $\mathfrak{H}$ is cyclic, and $\mathfrak{G} = \mathfrak{Q}\mathfrak{H}$.

Suppose, on $\{\pm e_1, \cdots, \pm e_n\}$, τ has orbits $O'_1, \cdots, O'_r$; they all have the same cardinality, $\langle \tau \rangle$ being normal in $\mathfrak{G}$.

Hence, $2n = r$ Card(O'_i). Either $r = 2n$, Card$(O'_i) = 1$, or $r = n$, Card(O'_i). Accordingly, either $\tau = 1$, $\mathfrak{G}$ is cyclic, or $\tau^2 = 1$, τ is central in $\mathfrak{G}$, and $\mathfrak{G}$ is commutative. In any case, $\mathfrak{G}$ is commutative, thus is simply transitive on $\{\pm e_1, \cdots, \pm e_n\}$, thus is cyclic of order $2n$. If σ is a generator of $\mathfrak{G}$, $\mathfrak{Q} = \langle \sigma^n \rangle$, and $\mathfrak{H} = \langle \sigma^2 \rangle$ is simply transitive on $\{e_1, \cdots, e_n\}$. The involution σ^n, commuting with σ^2, is a scalar matrix, i.e. $= -1$. But $-1 \notin \mathfrak{W}_1$. □

Proposition 9.5. *For any integer $n \geq 4$, if (B_{n-1}, α_{n-1}) is elliptic over η, so are (D_n, α_{n-1}), (D_n, α_n).*

Proof. This is clear, by comparing (3.1), 2) and 5). □

Proposition 9.6. *The pairs (D_5, α_4), (D_5, α_5) are elliptic over η.*

Proof. Because (B_4, α_4) is elliptic, (7.1), (7.3), (9.5). □

Proposition 9.7. *Suppose* char$(s) > 2$. *Then (D_6, α_5), (D_6, α_6) are elliptic over η if and only if* Card$(k(s)) \equiv 5$ *mod* 8.

Proof. Consider (D_6, α_6) only, the case of (D_6, α_5) being the same.

Let $\ell = \mathrm{char}(s)$. Note that the condition Card$(k(s)) \equiv 5$ mod 8 is equivalent to that $\ell \equiv 5$ mod 8, $[s : \mathbf{F}_\ell]$ is odd.

The subgroup $\mathfrak{G} = \langle \tau, \sigma \rangle$ of $\mathfrak{W}_1$,

$$\begin{cases} \tau : e_1 \mapsto e_2,\ e_2 \mapsto e_3,\ e_3 \mapsto e_4,\ e_4 \mapsto -e_1,\ e_5 \mapsto e_6,\ e_6 \mapsto -e_5 \\ \sigma : e_1 \mapsto e_2,\ e_2 \mapsto -e_3,\ e_3 \mapsto e_4,\ e_4 \mapsto e_1,\ e_5 \mapsto e_5,\ e_6 \mapsto -e_6 \end{cases}$$

is simply transitive on

$$X = \{s_1 e_1 + \cdots + s_6 e_6,\ s_i = 1, -1,\ s_1 \cdots s_6 = 1\}.$$

And

$$\tau^8 = 1,\ \sigma^8 = 1,\ \sigma\tau\sigma^{-1} = \tau^5.$$

If $\mathrm{Card}(k(s)) \equiv 5 \bmod 8$, $\mathfrak{G}$ is a quotient of $\pi_1^t(\eta, \overline{\eta})$, hence (D_6, α_6) is elliptic, (3.1), 5).

Next, suppose (D_6, α_6) is elliptic over η, and $\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{W}_1$ is a representation with monodromy $\mathfrak{G}$ transitive on X. The order $\mathrm{Card}(\mathfrak{G})$ is divisible by 32.

Base changing η to some η' of *odd* relative degree if necessary, one may assume $\mathfrak{G}$ is a 2-group, thus tame, with generators σ, τ, $\sigma\tau\sigma^{-1} = \tau^q$, $q = \mathrm{Card}(k(s))$.

Now, in $\mathrm{GL}_6(\mathbf{Z})$, no element has order 16, so $\tau^8 = \sigma^8 = 1$.

Write $P(T)$ for the characteristic polynomial of τ. As $\tau \in \mathfrak{W}_1$, $P(T)$ may be $(T^4+1)(T^2-1)$, $(T^4+1)(T^2+1)$, $(T^2+1)^2(T-1)^2$, $(T^2+1)^2(T+1)^2$, $(T^2+1)(T-1)(T+1)^3$, or $(T^2+1)(T+1)(T-1)^3$.

Show $P(T) \neq (T^4+1)(T^2-1)$:

Otherwise, say $\langle\tau\rangle$ normalizes $\{\pm e_1, \pm e_2, \pm e_3, \pm e_4\}$, and $\tau(e_5) = e_5$, $\tau(e_6) = -e_6$. By the relation $\sigma\tau\sigma^{-1} = \tau^q$, σ normalizes $\{\pm e_1, \cdots, \pm e_4\}$, $\{e_5, -e_5\}$, and $\{e_6, -e_6\}$. On $\{\pm e_1, \cdots, \pm e_4\}$, σ^2 being commutative with τ, equals some τ^i, $i = 2, 6$ (resp. $i = 4$), if σ is of order 8 (resp. 4). In either case, $\sigma^2 = \tau^i$ also on $\{\pm e_5, \pm e_6\}$. So $\sigma^2 = \tau^i$. But then $\mathfrak{G} = \langle\tau\rangle \cup \langle\tau\rangle\sigma$ is of order ≤ 16.

Show $P(T) \neq (T^2+1)(T-1)(T+1)^3$:

Otherwise, say τ normalizes $\{\pm e_1, \pm e_2\}$, $\tau(e_3) = e_3$, $\tau(e_i) = -e_i$, $i = 4, 5, 6$. The equation $\sigma\tau\sigma^{-1} = \tau^q$ implies that σ normalizes $\{\pm e_1, \pm e_2\}$, $\{e_3, -e_3\}$, and $\{\pm e_4, \pm e_5, \pm e_6\}$. But then σ has order ≤ 4, $\mathfrak{G}$ has order ≤ 16.

Similarly, $P(T) \neq (T^2+1)(T+1)(T-1)^3$.

Show $P(T) \neq (T^2+1)^2(T-1)^2$:

Otherwise, say τ normalizes $\{\pm e_1, \pm e_2\}$, $\{\pm e_3, \pm e_4\}$, and $\tau(e_5) = e_5$, $\tau(e_6) = e_6$. In particular, τ is of order 4. So σ must be of order 8, normalizes separately $\{\pm e_1, \pm e_2, \pm e_3, \pm e_4\}$ and $\{\pm e_5, \pm e_6\}$. Note that τ^2 commutes with σ, therefore, on $\{\pm e_1, \cdots, \pm e_4\}$, $\tau^2 = \sigma^4$, which clearly also holds on $\{\pm e_5, \pm e_6\}$. But then $\mathfrak{G} = \langle\sigma\rangle \cup \tau\langle\sigma\rangle \cup \tau^{-1}\langle\sigma\rangle$ has order ≤ 24.

Similarly, $P(T) \neq (T^2+1)^2(T+1)^2$.

So it can only be that $P(T) = (T^4+1)(T^2+1)$. Say τ normalizes separately $\{\pm e_1, \cdots, \pm e_4\}$ and $\{\pm e_5, \pm e_6\}$. Again, because of $\sigma\tau\sigma^{-1} = \tau^q$, $\{\pm e_1, \cdots, \pm e_4\}$ and $\{\pm e_5, \pm e_6\}$ are both normalized by σ. And σ is of order 8 or 4.

Show $q \equiv 5 \bmod 8$:

If $q \equiv 1 \bmod 8$, σ commutes with τ. So, on $\{\pm e_1, \cdots, \pm e_4\}$, $\sigma = \tau^i$, for some $i \in \mathbf{Z}/8\mathbf{Z}$. But then $\mathfrak{G} = \langle \sigma, \tau \rangle$ has 2 orbits on $\{\pm e_1 \pm e_2 \pm e_3 \pm e_4\}$, therefore has ≥ 2 orbits on X as well.

If $q \equiv 7 \bmod 8$, $\sigma\tau\sigma^{-1} = \tau^{-1}$. On $\{\pm e_1, \cdots, \pm e_4\}$, $\sigma^2 = 1$. So $\mathfrak{G}$ has 2 orbits on $\{\pm e_1 \pm e_2 \pm e_3 \pm e_4\}$, thus cannot be transitive on X.

If $q \equiv 3 \bmod 8$, σ is of order 4. On $\{\pm e_1, \cdots, \pm e_4\}$, $\sigma^2 = \tau^4$. So σ has characteristic polynomial either $(T^2+1)^2(T-1)^2$ or $(T^2+1)^2(T+1)^2$. In any case, $\sigma^2 = \tau^4$ also on $\{\pm e_5, \pm e_6\}$. But $\mathfrak{G} = \langle \tau \rangle \cup \langle \tau \rangle \sigma$ is of order ≤ 16. □

Proposition 9.8. *If* $\mathrm{char}(s) > 2$, (D_7, α_6), (D_7, α_7) *are not elliptic over* η.

Proof. Otherwise, there exists a representation $\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{W}_1$ whose image $\mathfrak{G}$ is transitive on the set of vectors

$$s_1 e_1 + \cdots + s_7 e_7,\ s_i \in \{1, -1\},\ s_1 \cdots s_7 = 1.$$

The quotient $\mathfrak{G}/\mathfrak{D}_1 \cap \mathfrak{G}$ is of order divisible by 16, for $\mathfrak{D}_1 \cap \mathfrak{G}$, being a sub-quotient of $\pi_1(\eta, \overline{\eta})$, has order ≤ 4. So, $\mathfrak{G}/\mathfrak{D}_1 \cap \mathfrak{G}$ contains a 2-Sylow subgroup of $\mathfrak{M} = \mathfrak{S}_7$, in particular, it contains a conjugate of $\langle (12), (34), (56) \rangle$. But $\langle (12), (34), (56) \rangle$ cannot be a sub-quotient of $\pi_1(\eta, \overline{\eta})$. □

Proposition 9.9. *If* $\mathrm{char}(s) > 2$, (D_8, α_7), (D_8, α_8) *are not elliptic over* η.

Proof. It suffices to consider (D_8, α_8). Suppose it is elliptic over η, $\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{W}_1$ is a representation with monodromy $\mathfrak{G}$ transitive on

$$\{s_1 e_1 + \cdots + s_8 \alpha_8,\ s_i = 1, -1,\ s_1 \cdots s_8 = 1\}.$$

Extending the base η if necessary, assume $\mathfrak{G}$ is a 2-group, in particular tame, with generators σ, τ, $\sigma\tau\sigma^{-1} = \tau^q$, $q = \mathrm{Card}(k(s))$.

Necessarily, $\tau^8 = \sigma^8 = 1$, since no element of $\mathrm{GL}_8(\mathbf{Z})$ of order 16 belongs to $\mathfrak{W}_1$. But then $\mathfrak{G}$ has order $\leq 64 < 2^7$. □

Proposition 9.10. *If* $\mathrm{char}(s) > 2$, $n \geq 9$, *then* (D_n, α_{n-1}), (D_n, α_n) *are not elliptic over* η.

Proof. It suffices to consider (D_n, α_n), which we assume is elliptic over η, and let $\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{W}_1$ be a representation whose monodromy $\mathfrak{G}$ acts transitively on

$$\{s_1 e_1 + \cdots + s_n e_n,\ s_i = 1, -1,\ s_1 \cdots s_n = 1\}.$$

Base changing η so that $\mathfrak{G}$ is a 2-group, of order divisible by 2^{n-1}. Then $\mathfrak{P} := \mathrm{Card}(\mathfrak{G}/\mathfrak{D}_1 \cap \mathfrak{G})$ is divisible by 2^{n-3}, for $\mathfrak{D}_1 \cap \mathfrak{G}$, being a sub-quotient of $\pi_1(\eta, \overline{\eta})$, is of order ≤ 4.

Now, $\mathrm{ord}_2(n!) \leq n-1$, and the equality holds if and only if n is a power of 2.

Hence, if n is not a power of 2, $\mathfrak{P}$ is of index ≤ 2 in a 2-Sylow subgroup of $\mathfrak{M} = \mathfrak{S}_n$, therefore some conjugate of $\langle (12), (34), (56), (78) \rangle$, say $\mathfrak{Q}$, satisfies $(\mathfrak{Q} : \mathfrak{Q} \cap \mathfrak{P}) \leq 2$. But $\mathfrak{Q} \cap \mathfrak{P}$ cannot be a sub-quotient of $\pi_1(\eta, \overline{\eta})$.

If n is a power of 2, thus $n \geq 16$, $\mathfrak{P}$ is of index ≤ 4 in a 2-Sylow subgroup of $\mathfrak{S}_n$, so a conjugate of $\langle (12), (34), \cdots, (n-1, n) \rangle$, say $\mathfrak{Q}$, satisfies $(\mathfrak{Q} : \mathfrak{Q} \cap \mathfrak{P}) \leq 4$. But $\mathfrak{Q} \cap \mathfrak{P}$ cannot be a sub-quotient of $\pi_1(\eta, \overline{\eta})$ either. □

10. Type ^2D

Let S, η, s be as in §4.

Let n be an integer ≥ 4. Write $n = 2^g r$, $g \geq 0$, r odd. Identify $\mathbf{Z}^n$ with $\mathbf{Z}^{2^g} \otimes_{\mathbf{Z}} \mathbf{Z}^r$, and the standard base $e_1, \cdots, e_n$ with $e'_1 \otimes e''_1, \cdots, e'_{2^g} \otimes e''_r$, where $e'_1, \cdots, e'_{2^g}$ (resp. $e''_1, \cdots, e''_r$) is the standard base of $\mathbf{Z}^{2^g}$ (resp. $\mathbf{Z}^r$).

Let $\mathfrak{W}$ denote the subgroup of $\mathrm{GL}_n(\mathbf{Z})$ generated by the diagonal matrices and monomial matrices.

Proposition 10.1. *A pair $(^2D_n, \alpha_1)$ over η, with ^2D_n unramified over S, is elliptic.*

Proof. The cyclic subgroup $\langle \sigma \rangle$ of $\mathfrak{W}$, where $\sigma : e_1 \mapsto e_2, \cdots, e_{n-1} \mapsto e_n, e_n \mapsto -e_1$, is simply transitive on $\{\pm e_1, \cdots, \pm e_n\}$, and is an unramified quotient of $\pi_1(\eta, \overline{\eta})$. So $(^2D_n, \alpha_1)$ is elliptic, (3.1), 9). □

Proposition 10.2. *If* $\mathrm{char}(s) > 2$, *any $(^2D_n, \alpha_1)$, with ^2D_n ramified over S, is elliptic.*

Proof. Define $\tau', \sigma' \in \mathrm{GL}_{2^g}(\mathbf{Z})$ by

$$\tau' : e'_1 \mapsto e'_2, \ \cdots, \ e'_{2^g-1} \mapsto e'_{2^g}, \ e'_{2^g} \mapsto -e'_1,$$

$$\sigma'\tau' = \tau'^{q^r}\sigma', \quad \sigma' : e'_1 \mapsto e'_1.$$

Write $q = \mathrm{Card}(k(s))$. Let $\tau \in \mathrm{GL}_n(\mathbf{Z})$ be such that

$$\tau : e'_i \otimes e''_j \mapsto \tau'^{q^{j-1}}(e'_i) \otimes e''_j,$$

for any $j = 1, \cdots, r$, and $i = 1, \cdots, 2^g$.

Let $\sigma \in \mathrm{GL}_n(\mathbf{Z})$ be such that

$$\sigma : e'_i \otimes e''_1 \mapsto e'_i \otimes e''_2,\ \cdots ,\ e'_i \otimes e''_{r-1} \mapsto e'_i \otimes e''_r,\ e'_i \otimes e''_r \mapsto \sigma'(e'_i) \otimes e''_1,$$

for any $i = 1, \cdots , 2^g$.

Clearly, τ is of order 2^{g+1}, $\sigma^r = \sigma' \otimes 1$, $\sigma\tau\sigma^{-1} = \tau^q$, $\langle \sigma, \tau \rangle$ is transitive on $\{\pm e_1, \cdots , \pm e_n\}$. Also, $\langle \sigma, \tau \rangle$ is a quotient of $\pi_1^t(\eta, \overline{\eta})$ lifting any given index of ${}^2D_n$. So $({}^2D_n, \alpha_1)$ is elliptic over η, (3.1), 9). □

Let $d \geq 1$, $f > 1$ be integers. Define pro-2-groups

$$F_1 = \langle x_1, \cdots , x_{d+2} |\ x_1^{2^f}[x_1, x_2][x_3, x_4] \cdots [x_{d+1}, x_{d+2}] = 1,\ d \text{ even} \rangle,$$

$$F_2 = \langle x_1, \cdots , x_{d+2} |\ x_1^2 x_2^4 [x_2, x_3] \cdots [x_{d+1}, x_{d+2}] = 1,\ d \text{ odd} \rangle,$$

$$F_3 = \langle x_1, \cdots , x_{d+2} |\ x_1^{2+2^f}[x_1, x_2][x_3, x_4] \cdots [x_{d+1}, x_{d+2}] = 1,\ d \text{ even} \rangle,$$

$$F_4 = \langle x_1, \cdots , x_{d+2} |\ x_1^2[x_1, x_2] x_3^{2^f}[x_3, x_4] \cdots [x_{d+1}, x_{d+2}] = 1,\ d \text{ even} \rangle,$$

where

$$[x, y] := x^{-1}y^{-1}xy$$

is the commutator.

If $\mathrm{char}(s) = 2$, recall that $\pi_1(\eta, \overline{\eta})$ has one of the groups $F_1, \cdots , F_4$ as the maximal pro-2 quotient, with $d = [\eta : \mathbf{Q}_2]$, and some integer f, cf. [3], p. 107-108.

Proposition 10.3. *If* $\mathrm{char}(s) = 2$*, any* $({}^2D_n, \alpha_1)$ *is elliptic over* η*.*

Proof. Define $a', b' \in \mathrm{GL}_{2^g}(\mathbf{Z})$ by

$$a : e'_1 \mapsto -e'_1,\ e'_i \mapsto e'_i,\ \forall\ i > 1,$$

$$b : e'_1 \mapsto e'_2,\ \cdots ,\ e'_{2^g-1} \mapsto e'_{2^g},\ e'_{2^g} \mapsto e'_1,$$

and $c'' \in \mathrm{GL}_r(\mathbf{Z})$ by

$$c'' : e''_1 \mapsto e''_2,\ \cdots ,\ e''_{r-1} \mapsto e''_r,\ e''_r \mapsto e''_1.$$

Let $a = a' \otimes 1, b = b' \otimes 1, c = 1 \otimes c'' \in \mathrm{GL}_n(\mathbf{Z})$. The group $\langle ab \rangle \times \langle c \rangle$ is simply transitive on $\{\pm e_1, \cdots , \pm e_n\}$.

To finish, it suffices to show either $\langle ab \rangle \times \langle c \rangle$ or $\langle a, b \rangle \times \langle c \rangle$ is a quotient of $\pi_1(\eta, \overline{\eta})$ lifting the given index of ${}^2D_n$.

As $\langle c \rangle$ is an unramified quotient of $\pi_1(\eta, \overline{\eta})$ of *odd* order, it even suffices to show that any given surjection $\chi : F \to \{1, -1\}$ lifts to a surjection $\rho : F \to \langle ab \rangle$ or a surjection $\rho : F \to \langle a, b \rangle$, where F is the maximal pro-2-quotient of $\pi_1(\eta, \overline{\eta})$.

The verification is straightforward from the structure of F. For instance, consider $g \geq 2$, and $F = \langle x, y, z | x^2 y^4 [y, z] = 1 \rangle$. According to the values of (x, y, z) in $\{1, -1\}$, define $\rho : F \to \langle a, b \rangle$ as :

1) $(-1, 1, 1)$, let $\rho : (x, y, z) \mapsto (a, 1, b)$.

2) $(1,-1,1)$, let $\rho:(x,y,z)\mapsto((ab)^{-2},ab,1)$.

3) $(1,1,-1)$, let $\rho:(x,y,z)\mapsto(1,1,ab)$.

4) $(-1,1,-1)$, let $\rho:(x,y,z)\mapsto(a,1,ab)$.

5) $(1,-1,-1)$, let $\rho:(x,y,z)\mapsto((ab)^{-2},ab,ab)$.

6) $(-1,-1,1)$, let $\rho:(x,y,z)\mapsto(a,ab,ab^2ab^{-2})$, if $g=2$, and $\rho:(x,y,z)\mapsto(ab^2,ab^{-1},ab^3ab^{-3})$, if $g>2$.

7) $(-1,-1,-1)$, let $\rho:(x,y,z)\mapsto(ab^2,ab,ab^{-1})$, if $g=2$, and $\rho:(x,y,z)\mapsto(b^{-1}ab^2aba,ab^{-1},ab)$, if $g>2$. □

11. Type E_6

Let E be a 6-dimensional $\mathbf{F}_2$-vector space of base e_i, f_j, $1\le i,j\le 3$, $V_i=\mathbf{F}_2e_i+\mathbf{F}_2f_i$, $i=1,2,3$, and q the quadratic form on E such that

$$q(e_i)=q(f_j)=1\ ,\ q(e_i+e_j)=q(f_i+f_j)=0\ ,\ q(e_i+f_j)=\delta_{ij}$$

where $\delta_{ij}=1$, if $i=j$, and 0, if $i\neq j$, $\forall\ i,j=1,2,3$.

Let X be the set

$$\{v\in E\backslash\{0\},\ q(v)=0\}$$

of non-zero singular vectors in E.

In view of (3.1), 6), we need to determine up to conjugation the solvable subgroups of $\mathrm{O}(q)$ that are transitive on X.

The group $\mathrm{O}(q)$ is of order $2^7.3^4.5$, and X has 27 elements consisting of the vectors v_i+v_j, where $v_i\in V_i$, $v_j\in V_j$, $i\neq j$, $v_i,v_j\neq 0$. Clearly, every 3-Sylow subgroup of $\mathrm{O}(q)$ is transitive on X.

Note that V_i being an elliptic plane, $\mathrm{O}(q|V_i)=\mathrm{GL}(V_i)=\langle\gamma_i,\tau_i\rangle$, where

$$\gamma_i:\begin{cases} e_i\mapsto f_i\\ f_i\mapsto e_i+f_i\end{cases},\ \tau_i:\begin{cases} e_i\mapsto f_i\\ f_i\mapsto e_i\end{cases}$$

The planes V_i are permuted by $\langle\gamma,\tau\rangle\le\mathrm{O}(q)$, where

$$\gamma:\begin{cases} e_1\mapsto e_2,\ e_2\mapsto e_3,\ e_3\mapsto e_1\\ f_1\mapsto f_2,\ f_2\mapsto f_3,\ f_3\mapsto f_1\end{cases},\ \tau:\begin{cases} e_1\mapsto e_1,\ e_2\mapsto e_3,\ e_3\mapsto e_2\\ f_1\mapsto f_1,\ f_2\mapsto f_3,\ f_3\mapsto f_2\end{cases}$$

Let

$$\mathfrak{P}:=\langle\gamma,\gamma_1,\gamma_2,\gamma_3\rangle,$$

which is a 3-Sylow subgroup of $\mathrm{O}(q)$.

Put $\gamma_0=\gamma_1\gamma_2\gamma_3$, $\tau_0=\tau_1\tau_2\tau_3$.

The group $\mathfrak{P}$ has center

$$\mathfrak{Z}=\langle\gamma_0\rangle,$$

derived group

$$\mathfrak{D} = \langle \gamma_1\gamma_2^{-1}, \gamma_2\gamma_3^{-1} \rangle,$$

and maximal subgroups

$$\mathfrak{M} = \langle \gamma_1, \gamma_2, \gamma_3 \rangle,\ \mathfrak{M}_i = \langle \mathfrak{D}, \gamma\gamma_1^i \rangle,\quad i \in \mathbf{Z}/3\mathbf{Z}.$$

Note that

$$\tau\mathfrak{M}_1\tau^{-1} = \mathfrak{M}_2.$$

For any $i \in \mathbf{Z}/3\mathbf{Z}$,

$$\mathfrak{Z} = [\mathfrak{M}_i, \mathfrak{M}_i].$$

The subgroups of $\mathfrak{P}$ that are transitive on X are $\mathfrak{P}$, $\mathfrak{M}_i$, $i \in \mathbf{Z}/3\mathbf{Z}$.

Denote by $\mathfrak{Q}$ the subgroup of $\mathrm{O}(q) \cap \mathrm{GL}_3(E)$ consisting of those elements g such that $g(e_2 + e_3) = e_2 + e_3$, and

$$g(e_1) = e_1 + b(e_2 + e_3),\ b \in \mathbf{F}_2[\mathfrak{Z}].$$

One calculates that

$$\mathfrak{Q} = \{1, \tau, \gamma_1^i\tau_0^j\beta\tau_0^{-j}\gamma_1^{-i},\ i \in \mathbf{Z}/3\mathbf{Z},\ j \in \mathbf{Z}/2\mathbf{Z}\},$$

where

$$\beta : \begin{cases} e_1 \mapsto e_1 + e_2 + e_3 \\ e_2 \mapsto e_1 + \gamma_0 e_2 + \gamma_0^{-1} e_3 \\ e_3 \mapsto e_1 + \gamma_0^{-1} e_2 + \gamma_0 e_3 \end{cases}$$

Lemma 11.1. *For any subgroup $\mathfrak{S}$ of $\mathrm{O}(q)$, let its normalizer in $\mathrm{O}(q)$ be denoted by $N(\mathfrak{S})$. Then*

1) $N(\mathfrak{M}) = \langle \mathfrak{P}, \tau, \tau_1, \tau_2, \tau_3 \rangle$.

2) $N(\mathfrak{D}) = N(\mathfrak{P}) = \mathfrak{P}\langle \tau, \tau_0 \rangle$.

3) $N(\mathfrak{M}_1) = N(\mathfrak{M}_2) = \mathfrak{P}\langle \tau\tau_0 \rangle$.

4) $N(\mathfrak{Z}) = N(\mathfrak{M}_0) = \mathfrak{P}\mathfrak{Q}\langle \tau_0 \rangle$.

Proof. Note that the planes V_1, V_2, V_3 are all the irreducible sub-$\mathfrak{M}$-modules of E. So $N(\mathfrak{M})$ permutes them.

Each V_i, $i = 1, 2, 3$, has

$$\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3) = \langle \mathfrak{M}, \tau_1, \tau_2, \tau_3 \rangle$$

as its normalizer in $\mathrm{O}(q)$. Thus,

$$N(\mathfrak{M}) = \langle \mathfrak{M}, \tau_1, \tau_2, \tau_3, \gamma, \tau \rangle = \langle \mathfrak{P}, \tau, \tau_1, \tau_2, \tau_3 \rangle.$$

This is 1).

As $\mathfrak{D}$-modules, V_i, $i = 1, 2, 3$, are also irreducible. From

$$V_1 = \mathrm{Ker}(\gamma_2\gamma_3^{-1} - 1),\ V_2 = \mathrm{Ker}(\gamma_1\gamma_3^{-1} - 1),\ V_3 = \mathrm{Ker}(\gamma_1\gamma_2^{-1} - 1),$$

it follows that

$$\mathrm{GL}_{\mathfrak{D}}(E) = \langle \gamma_1, \gamma_2, \gamma_3 \rangle = \mathfrak{M}.$$

As $\mathfrak{M} = \mathrm{GL}_{\mathfrak{D}}(E)$ is normalized by $N(\mathfrak{D})$, $N(\mathfrak{D})$ is contained in $N(\mathfrak{M}) = \langle \mathfrak{P}, \tau, \tau_1, \tau_2, \tau_3 \rangle$.

By inspection, $N(\mathfrak{D}) = \langle \mathfrak{P}, \tau, \tau_0 \rangle$; this group normalizes $\mathfrak{P}$, hence $N(\mathfrak{P}) = N(\mathfrak{D})$. This proves 2).

In either group $\mathfrak{M}_i$, $i = 1, 2$, $\mathfrak{D}$ is the only non-cyclic subgroup of order 9. Therefore, $N(\mathfrak{M}_i) \le N(\mathfrak{D}) = \langle \mathfrak{P}, \tau, \tau_0 \rangle$, and both are equal to $\mathfrak{P}\langle \tau\tau_0 \rangle$, as one verifies. This shows 3).

Finally, $N(\mathfrak{Z})$ is generated by τ_0 and $\mathrm{O}(q) \cap \mathrm{GL}_{\mathfrak{Z}}(E)$.

But, $\mathrm{O}(q) \cap \mathrm{GL}_{\mathfrak{Z}}(E) = \mathfrak{P}\mathfrak{Q}$: $\forall\, g \in \mathrm{O}(q) \cap \mathrm{GL}_{\mathfrak{Z}}(E)$, as $\mathfrak{P}$ is transitive on X, $\exists\, p \in \mathfrak{P}$, $p^{-1}g(e_2 + e_3) = e_2 + e_3$.

The vector $p^{-1}g(e_1)$, orthogonal to $p^{-1}g(e_2 + e_3)$ and $p^{-1}g(f_2 + f_3)$, is of the form

$$p^{-1}g(e_1) = ae_1 + b(e_2 + e_3),\ a \in \mathfrak{Z},\ b \in \mathbf{F}_2[\mathfrak{Z}]$$

Say, $a = \gamma_0^i$, $i \in \mathbf{Z}/3\mathbf{Z}$. Then

$$\gamma_1^{-i} p^{-1} g : \begin{cases} e_2 + e_3 \mapsto e_2 + e_3 \\ e_1 \mapsto e_1 + b(e_2 + e_3) \end{cases}$$

Namely, $\gamma_1^{-i} p^{-1} g \in \mathfrak{Q}$, and $g \in p\gamma_1^i \mathfrak{Q} \subset \mathfrak{P}\mathfrak{Q}$.

Now, $\mathfrak{P}, \tau_0, \beta$ do normalize $\mathfrak{M}_0$. Hence, $N(\mathfrak{M}_0) = N(\mathfrak{Z}) = \mathfrak{P}\mathfrak{Q}\langle \tau_0 \rangle$, which is 4). □

Suppose given a solvable subgroup $\mathfrak{G}$ of $\mathrm{O}(q)$ transitive on X. By conjugation in $\mathrm{O}(q)$, one arranges so that $\mathfrak{G} \cap \mathfrak{P}$ is a 3-Sylow subgroup of $\mathfrak{G}$.

Necessarily, $\mathfrak{G} \cap \mathfrak{P} = \mathfrak{P}$, or $\mathfrak{M}_i$, $i \in \mathbf{Z}/3\mathbf{Z}$.

Lemma 11.2. $5 \nmid \mathrm{Card}(\mathfrak{G})$.

Proof. Let $\mathfrak{L}$ be a $(3,5)$-Hall subgroup of $\mathfrak{G}$ containing $\mathfrak{G} \cap \mathfrak{P}$.

We need to show $\mathfrak{L} = \mathfrak{G} \cap \mathfrak{P}$.

The group $\mathfrak{G} \cap \mathfrak{P}$ is normal in $\mathfrak{L}$, for 5 is not congruent to 1 modulo 3, and if $\mathrm{Card}(\mathfrak{G} \cap \mathfrak{P}) = 27$, lies even in the center of $\mathfrak{L}$, for 1 is only divisor of 27 that is congruent to 1 modulo 5.

Now, note that the normalizer of $\mathfrak{P}$ and the centralizers of $\mathfrak{M}_i$, $i \in \mathbf{Z}/3\mathbf{Z}$, all normalizing $\mathfrak{D}$, have order dividing $3^4.2^2$, (11.1), 2). □

Lemma 11.3. *If $\mathfrak{A}$ is a maximal abelian normal subgroup of $\mathfrak{G}$, then* $2 \nmid \mathrm{Card}(\mathfrak{A})$.

Proof. Denote by $\mathfrak{a}$ the 2-Sylow subgroup of $\mathfrak{A}$. The space $E^{\mathfrak{a}}$ is a non-zero $\mathfrak{G}$-module, in particular, a non-zero $\mathfrak{D}$-module, hence, $q|E^{\mathfrak{a}}$ is non-degenerate.

Now, $\mathfrak{a}$ normalizes $(E^{\mathfrak{a}})^{\perp}$, and

$$((E^{\mathfrak{a}})^{\perp})^{\mathfrak{a}} \subset E^{\mathfrak{a}} \cap (E^{\mathfrak{a}})^{\perp} = 0.$$

So $(E^{\mathfrak{a}})^{\perp} = 0$, because $\mathfrak{a}$ is a 2-group. Thus, $E^{\mathfrak{a}} = E$, $\mathfrak{a} = 1$. □

Therefore, a maximal abelian normal subgroup $\mathfrak{A}$ of $\mathfrak{G}$ is a 3-group, of order $27, 9$, or 3.

If $\mathrm{Card}(\mathfrak{A}) = 27$, $\mathfrak{A} = \mathfrak{M}$.

Then $\mathfrak{G}$ is contained in $N(\mathfrak{M}) = \langle \mathfrak{P}, \tau, \tau_1, \tau_2, \tau_3 \rangle$, and has the form $\mathfrak{M}\mathfrak{H}$, where $\mathfrak{H}$ is any subgroup of $\langle \gamma, \tau, \tau_1, \tau_2, \tau_3 \rangle$ containing γ. Explicitly, if $\mathfrak{T}$ denotes any of the groups

$$1,\ \langle \tau \rangle,\ \langle \tau_0 \rangle,\ \langle \tau\tau_0 \rangle,\ \langle \tau, \tau_0 \rangle,$$

then $\mathfrak{H} = \langle \gamma \rangle \mathfrak{T}$, $\langle \gamma, \tau_1\tau_2, \tau_2\tau_3 \rangle \mathfrak{T}$.

Next, suppose $\mathfrak{A}$ cyclic of order 9.

Then, $\mathfrak{A}$ is irreducible on E, and is its own centralizer in $\mathrm{O}(q)$. Because the quotient $N(\mathfrak{A})/\mathfrak{A}$ acts faithfully by conjugation on $\mathfrak{A}$, and because $\mathrm{Aut}(\mathfrak{A}) \simeq (\mathbf{Z}/9\mathbf{Z})^{\times} = \mathbf{Z}/6\mathbf{Z}$, the normalizer $N(\mathfrak{A})$ has order dividing $3^3.2$. Hence, $(N(\mathfrak{A}) : \mathfrak{G} \cap \mathfrak{P}) \le 2$, and $\mathfrak{G} \cap \mathfrak{P}$ is normal in $N(\mathfrak{A})$. It can only be that $\mathfrak{G} \cap \mathfrak{P} = \mathfrak{M}_1$ or $\mathfrak{M}_2 = \tau \mathfrak{M}_1 \tau^{-1}$. And, $\mathfrak{G}$ is conjugate to $\mathfrak{M}_1$ or $\mathfrak{M}_1 \langle \tau\tau_0 \rangle$.

Next, suppose $\mathfrak{A} \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

Then $\mathfrak{A}$ is conjugate to $\mathfrak{D}$, and $\mathfrak{G}$ is conjugate to a subgroup of $N(\mathfrak{D})$. Using that $N(\mathfrak{D})/\mathfrak{D} \simeq \mathfrak{S}_3 \times \mathfrak{S}_3$, the two factors being $\langle \gamma, \tau \rangle$ and $\langle \gamma_1, \tau_0 \rangle$ ($[\gamma, \gamma_1] \in \mathfrak{D}$), one finds that $\mathfrak{G}$ is conjugate to $\mathfrak{M}_1$, or $\langle \mathfrak{M}_1, \tau\tau_0 \rangle$, or $\mathfrak{M}_0 \mathfrak{T}$, where $\mathfrak{T} = 1, \langle \tau \rangle, \langle \tau_0 \rangle, \langle \tau\tau_0 \rangle, \langle \tau, \tau_0 \rangle$.

Finally, suppose $\mathrm{Card}(\mathfrak{A}) = 3$.

Then, $\mathfrak{A} = \mathfrak{Z}$, and $\mathfrak{G} \le N(\mathfrak{Z}) = N(\mathfrak{M}_0)$. In this case, one checks that $\mathfrak{G}$ is conjugate to $\mathfrak{M}_0 \langle \beta \rangle$, $\mathfrak{M}_0 \langle \beta, \tau_0 \rangle$, $\mathfrak{M}_0 \mathfrak{Q}$, $\mathfrak{M}_0 \mathfrak{Q} \langle \tau_0 \rangle$, $\mathfrak{P}\mathfrak{Q}$, or $\mathfrak{P}\mathfrak{Q}\langle \tau_0 \rangle$.

We have obtained

Proposition 11.4. *Let $\mathfrak{T}$ be any of the groups $1, \langle \tau \rangle, \langle \tau_0 \rangle, \langle \tau\tau_0 \rangle, \langle \tau, \tau_0 \rangle$. Then the solvable subgroups of $\mathrm{O}(q)$ transitive on X are the conjugates of $\mathfrak{P}\mathfrak{T}$, $\langle \mathfrak{P}, \tau_1\tau_2, \tau_2\tau_3 \rangle \mathfrak{T}$, $\mathfrak{P}\mathfrak{Q}$, $\mathfrak{P}\mathfrak{Q}\langle \tau_0 \rangle$, $\mathfrak{M}_0 \mathfrak{T}$, $\mathfrak{M}_0 \langle \beta \rangle$, $\mathfrak{M}_0 \langle \beta, \tau_0 \rangle$, $\mathfrak{M}_0 \mathfrak{Q}$, $\mathfrak{M}_0 \mathfrak{Q} \langle \tau_0 \rangle$, $\mathfrak{M}_1$, $\mathfrak{M}_1 \langle \tau\tau_0 \rangle$.*

Proposition 11.5. *Let S, η, s be as in §4. The pairs (E_6,α_1), (E_6,α_6) are elliptic over η if and only if either s is of characteristic 3 or $\mathrm{Card}(k(s)) \equiv \pm 4$ mod 9.*

Proof. By (3.1), 6), (E_6,α_1), (E_6,α_6) are elliptic over η if and only if some group in the previous proposition is a quotient of $\pi_1(\eta,\overline{\eta})$.

If s is of characteristic 3, either $\mathfrak{M}_0$ or $\mathfrak{M}_1$ is a quotient of $\pi_1(\eta,\overline{\eta})$. Indeed, let P denote a maximal pro-3 quotient of $\pi_1(\eta,\overline{\eta})$.

When $\mu_3(\eta) = 1$, P is a free pro-3-group of rank ≥ 2, thus has a quotient isomorphic to $\mathfrak{M}_1$.

When $\mu_3(\eta) > 1$, P has the presentation

$$\langle x_1,\cdots,x_{d+2} \mid x_1^q[x_1,x_2][x_3,x_4]\cdots[x_{d+1},x_{d+2}] = 1\rangle$$

where $d = [\eta : \mathbf{Q}_3]$, q is the maximal power of 3 such that $\mu_q(\eta) = \mu_q(\overline{\eta})$, and $[x,y] := x^{-1}y^{-1}xy$ is the commutator of x, y. The homomorphism

$$\begin{cases} x_1 \mapsto \gamma \\ x_2 \mapsto \gamma_0 \\ x_3 \mapsto \gamma_1\gamma_2^{-1} \\ x_i \mapsto 1,\ i > 3 \end{cases}$$

$P \to \mathfrak{M}_0$ is clearly surjective.

Suppose s is not of characteristic 3. Then $\mathfrak{M}_0$ is not a sub-quotient of $\pi_1(\eta,\overline{\eta})$. This excludes all but $\mathfrak{M}_1$, $\mathfrak{M}_1\langle\tau\tau_0\rangle$ in the list of (11.4).

Any quotient $\rho : \pi_1(\eta,\overline{\eta}) \to \mathfrak{M}_1$ (resp. $\rho : \pi_1(\eta,\overline{\eta}) \to \mathfrak{M}_1\langle\tau\tau_0\rangle$) is necessarily tame with cyclic ramification group of order 9 ; from the structure of $\pi_1^t(\eta,\overline{\eta})$, it follows easily that such ρ exists if and only if $\mathrm{Card}(k(s)) \equiv 4$ mod 9 (resp. $\mathrm{Card}(k(s)) \equiv -4$ mod 9.) □

12. Type E_7

Let $E, (,)$ be a 6-dimensional symplectic $\mathbf{F}_2$-vector space, e_i, f_j, $1 \leq i,j \leq 3$, a sympletic base.

Let q be the quadratic form on E such that

$$q(e_i) = q(f_j) = 1,\ q(e_i+e_j) = q(f_i+f_j) = 0,\ q(e_i+f_j) = \delta_{ij}$$

where $\delta_{ij} = 1$, if $i = j$, and 0, if $i \neq j$, $\forall\ i,j = 1,2,3$.

Then, $\mathrm{O}(q)$ is a subgroup of $\mathrm{Sp}(E)$.

Let the quotient $\mathrm{Sp}(E)/\mathrm{O}(q)$ be denoted by X; it has 28 elements, as $\mathrm{Card}(\mathrm{Sp}(E)) = 2^9.3^4.5.7$, $\mathrm{Card}(\mathrm{O}(q)) = 2^7.3^4.5$.

We determine up to conjugation the solvable subgroups of $\mathrm{Sp}(E)$ that are transitive on X, cf. (3.1), 7).

Any such subgroup contains a 7-Sylow subgroup of $\mathrm{Sp}(E)$. By conjugation in $\mathrm{Sp}(E)$, we suppose it contains ζ, where

$$\zeta : \begin{cases} e_1 \mapsto e_2,\ e_2 \mapsto e_3,\ e_3 \mapsto e_1 + e_2 \\ f_1 \mapsto f_1 + f_2,\ f_2 \mapsto f_3,\ f_3 \mapsto f_1 \end{cases}$$

Indeed, ζ is of order 7, because letting $V = \mathbf{F}_2 e_1 + \mathbf{F}_2 e_2 + \mathbf{F}_2 e_3$, $V^\vee = \mathbf{F}_2 f_1 + \mathbf{F}_2 f_2 + \mathbf{F}_2 f_3$, then

$$\det(T - \zeta, V) = T^3 + T + 1\ ,\ \det(T - \zeta, V^\vee) = T^3 + T^2 + 1$$

and

$$\det(T - \zeta, E) = (T^3 + T + 1)(T^3 + T^2 + 1) = (T^7 - 1)/(T - 1).$$

As ζ-modules, $V, V^\vee$ are irreducible, mutually non-isomorphic. So, $0, V, V^\vee, E$ are the only sub-ζ-modules of E.

The commutant $\mathrm{End}_\zeta(E)$ equals

$$\mathbf{F}_2[\zeta|V] \times \mathbf{F}_2[\zeta|V^\vee],$$

and

$$\mathrm{GL}_\zeta(E) \cap \mathrm{Sp}(E) = \mathbf{F}_2[\zeta]^\times = \langle\zeta\rangle.$$

That is to say, $\langle\zeta\rangle$ is its own centralizer in $\mathrm{Sp}(E)$.

The normalizer of $\langle\zeta\rangle$ in $\mathrm{Sp}(E)$ has generators ζ, σ, with

$$\sigma : \begin{cases} e_1 \mapsto f_1,\ e_2 \mapsto f_2,\ e_3 \mapsto f_2 + f_3 \\ f_1 \mapsto e_1,\ f_2 \mapsto e_2 + e_3,\ f_3 \mapsto e_3 \end{cases}$$

for, this normalizer modulo $\langle\zeta\rangle$ acts faithfully by conjugation on $\langle\zeta\rangle$, and σ satisfies

$$\sigma^6 = 1,\ \sigma\zeta\sigma^{-1} = \zeta^{-2}.$$

Let $\mathfrak{S}$ be the centralizer of V in $\mathrm{Sp}(E)$.

Via $g \mapsto (g-1)|V^\vee$, $\mathfrak{S}$ can be identified with the $\mathbf{F}_2$-vector space of linear transformations $A : V^\vee \to V$ such that the bilinear form

$$x, y \mapsto (x, Ay)$$

is symmetric in $x, y \in V^\vee$.

Since for any $g \in \mathfrak{S}$, the function $z \mapsto (z, (g-1)z)$ is linear on $V^\vee$, there is a unique vector $v_g \in V$ satisfying $(z, (g-1)z) = (v_g, z)$, $\forall\ z \in V^\vee$.

The function $\mathfrak{S} \to V$, $g \mapsto v_g$, is linear; its kernel $\mathfrak{S}^1$ consists of those elements $g \in \mathfrak{S}$ such that the form $x, y \mapsto (x, (g-1)y)$ is alternating, i.e. $(x, (g-1)y) = (x \wedge y, \omega_g)$, for some $\omega_g \in \wedge^2 V$. The map $g \mapsto \omega_g$ establishes a canonical isomorphism from $\mathfrak{S}_1$ onto $\wedge^2 V$.

The sequence

$$0 \to \mathfrak{S}^1 \to \mathfrak{S} \xrightarrow{g \mapsto v_g} V \to 0$$

is exact.

Now, $\wedge^2 V, V$ being distinct as ζ-modules, $\mathfrak{S}$ splits uniquely,

$$\mathfrak{S} = \mathfrak{S}^1 \oplus \mathfrak{S}^2$$

with $\mathfrak{S}^2$ ζ-linearly isomorphic to V.

Proposition 12.1. *The solvable subgroups of* $\mathrm{Sp}(E)$ *that are transitive on* X *are the conjugates of* $\langle\zeta\rangle\mathfrak{S}$*,* $\langle\zeta,\sigma^2\rangle\mathfrak{S}$*,* $\langle\zeta\rangle\mathfrak{S}^i$*,* $\langle\zeta,\sigma^2\rangle\mathfrak{S}^i$*,* $i = 1, 2$.

Proof. Suppose $\mathfrak{G} \leq \mathrm{Sp}(E)$ solvable, transitive on X, and $\zeta \in \mathfrak{G}$.

Recall that $\mathrm{Card}(\mathrm{Sp}(E)) = 2^9.3^4.5.7$, $\mathrm{Card}(\mathrm{O}(q)) = 2^7.3^4.5$.

One has $5 \nmid \mathrm{Card}(\mathfrak{G})$, for otherwise $\mathfrak{G}$ had a Hall subgroup of order 35, necessarily cyclic. But $\mathbf{Z}/35\mathbf{Z}$ has no faithful 6-dimensional representations over $\mathbf{F}_2$.

Write $\mathrm{Card}(\mathfrak{G}) = 2^i.3^j.7$, $i \geq 2$, $j \geq 0$.

Let $\mathfrak{L}$ be a Hall subgroup of $\mathfrak{G}$, of order $3^j.7$, containing ζ.

Since $j \leq 4$, $\langle\zeta\rangle$ is normal in $\mathfrak{L}$. So $\mathfrak{L} \leq \langle\zeta,\sigma\rangle$. Either $\mathfrak{L} = \langle\zeta\rangle$ or $\langle\zeta,\sigma^2\rangle$, and $j = 0$ or 1.

Then, let $\mathfrak{H}$ be a Hall subgroup of $\mathfrak{G}$, of order $2^i.7$, containing ζ.

As $i \geq 2$, $\mathfrak{H}$ is not contained in $\langle\zeta,\sigma\rangle$, i.e. $\langle\zeta\rangle$ is not normal in $\mathfrak{H}$.

Let $\mathfrak{A}$ be a maximal abelian normal subgroup of $\mathfrak{H}$.

One has $7 \nmid \mathrm{Card}(\mathfrak{A})$, since otherwise the unique 7-Sylow subgroup of $\mathfrak{A}$ would be normal in $\mathfrak{H}$.

Thus, $\mathfrak{A}$ is a 2-group.

Then $E^{\mathfrak{A}}$, the subspace of E centralized by $\mathfrak{A}$, is a non-zero $\mathfrak{H}$-module, and being normalized by ζ, it is equal to V or $V^\vee$.

Replacing $\mathfrak{G}$ by $\sigma\mathfrak{G}\sigma^{-1}$ if necessary, assume $E^{\mathfrak{A}} = V$.

Now, $\mathfrak{A} \leq \mathfrak{S}$, and as σ^3 does not normalize V, $\sigma^3 \notin \mathfrak{H}$, and $\mathfrak{H} \cap \langle\zeta,\sigma\rangle = \langle\zeta\rangle$.

The group $\mathfrak{H}$ has $2^\alpha = \mathrm{Card}(\mathfrak{H}/\langle\zeta\rangle)$ 7-Sylow subgroups, and only one 2-Sylow subgroup, because $2^\alpha.7 - 2^\alpha(7-1) = 2^\alpha$. If $\mathfrak{a} \leq \mathfrak{H}$ is this 2-Sylow subgroup, $E^{\mathfrak{a}}$ is a non-zero sub-$\mathfrak{H}$-module of $E^{\mathfrak{A}} = V$. So $E^{\mathfrak{a}} = V$, $\mathfrak{a} \leq \mathfrak{S}$, $\mathfrak{a}$ is abelian. So $\mathfrak{A} = \mathfrak{a}$ is 2-Sylow in $\mathfrak{H}$, by the choice of $\mathfrak{A}$.

One finds that $\mathfrak{H} \leq \langle\zeta\rangle\mathfrak{S}$, and $\mathfrak{G} = \mathfrak{L}\mathfrak{H} \leq \langle\zeta,\sigma^2\rangle\mathfrak{S}$.

To finish, it needs to show that $\langle\zeta\rangle\mathfrak{S}^i$, $i = 1, 2$, are both transitive on X.

Any $g \in \mathfrak{S}$ has the form

$$g : \begin{cases} e_i \mapsto e_i \ , \ i = 1, 2, 3 \\ f_i \mapsto f_i + \sum_{j=1,2,3} A_{ji} e_j \end{cases}$$

where (A_{ij}) is a symmetric matrix with coefficients in $\mathbf{F}_2$. This g preserves the quadratic form q if and only if $A_{12} = A_{23} = A_{13}$.

The elements of $\mathfrak{S}^1$ correspond to those (A_{ij}) with zero diagonal entries.

So, $\mathrm{O}(q) \cap \langle\zeta\rangle\mathfrak{S}^1 = \mathrm{O}(q) \cap \mathfrak{S}^1 = \{1, g_1\}$, where

$$g_1 : \begin{cases} e_i \mapsto e_i, \ i = 1, 2, 3 \\ f_1 \mapsto f_1 + e_2 + e_3, \ f_2 \mapsto f_2 + e_1 + e_3, \ f_3 \mapsto f_3 + e_1 + e_2 \end{cases}$$

A simple calculation shows that $\mathfrak{S}^2$ is spanned as a ζ-module by τ,

$$\tau \ : \begin{cases} e_i \mapsto e_i, \ i = 1, 2, 3 \\ f_1 \mapsto f_1 + e_1, \ f_2 \mapsto f_2 + e_3, \ f_3 \mapsto f_3 + e_2 \end{cases}$$

and $\mathrm{O}(q) \cap \langle\zeta\rangle\mathfrak{S}^2 = \mathrm{O}(q) \cap \mathfrak{S}^2$ consists of 1, and $g_2 := \zeta^2 \tau \zeta^{-2}$. Explicitly,

$$g_2 : \begin{cases} e_i \mapsto e_i, \ i = 1, 2, 3 \\ f_1 \mapsto f_1 + e_2 + e_3, \ f_2 \mapsto f_2 + e_1 + e_3, \ f_3 \mapsto f_3 + e_1 + e_2 + e_3 \end{cases}$$

As $\mathrm{Card}(X) = 28$, $\mathrm{Card}(\langle\zeta\rangle\mathfrak{S}^i) = 56$, $i = 1, 2$, both $\langle\zeta\rangle\mathfrak{S}^i$ are indeed transitive on X. □

Proposition 12.2. *Let S, η, s be as in §4. The pair (E_7, α_7) is elliptic over η if and only if s is of characteristic* 2.

Proof. Any solvable subgroup $\boldsymbol{\mathfrak{G}}$ of $\{1, -1\} \times \mathrm{Sp}(E)$ transitive on

$$\{1, -1\} \times (\mathrm{Sp}(E)/\mathrm{O}(q))$$

contains an $\mathbf{F}_2^4$ (12.1). Only if s is of characteristic 2, $\boldsymbol{\mathfrak{G}}$ may be a quotient of $\pi_1(\eta, \overline{\eta})$.

If s is of characteristic 2, $\{1, -1\} \times \langle\zeta\rangle\mathfrak{S}$ is a quotient of $\pi_1(\eta, \overline{\eta})$, by (4.1) and that $\langle\zeta\rangle\mathfrak{S}$ has no subgroup of index 2. One finishes by (3.1), 7). □

References

1. D. Livingstone and A. Wagner. Transitivity of finite permutation groups on unordered sets. Math. Z, 90 : 393–403, 1965.
2. V. Kumar Murty and Vijay. M. Patankar. Splitting of abelian varieties. Int. Math. Res. Not, 2008.
3. J.P. Serre. Cohomologie Galoisienne. LNM 5, cinquième edition, 1997.
4. J. Tate. Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T.Honda). Séminaire Bourbaki, 1968/69, Exp. 352, LNM 179 : 95–110, 1971.

Department of Mathematics, University of Toronto
E-mail address: murty@math.toronto.edu, zongying@math.toronto.edu